

Data Protection Act (2021 Revision)

Guide for Data Controllers

Introduction

Note: This guidance is based on the United Kingdom's Information Commissioner's Office's Guide to the General Data Protection Regulation (GDPR), available at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>.

The Data Protection Act (2021 Revision) (the "DPA") is a powerful piece of legislation. It introduces globally recognized principles about the use of personal data to the Cayman Islands. The DPA aligns the Cayman Islands with other major jurisdictions around the world, notably the European Union, and thereby facilitates the free flow of data – a pre-requisite for the Cayman Islands being an equal and competitive participant in today's globalized economy.

Moreover, the DPA provides a standard framework for both public and private entities in the management of the personal data they use. Internationally active organisations will find many similarities between the data protection act of the Cayman Islands and of other jurisdictions where they are active. The DPA aims to reduce the administrative burden of operating internationally and cement the Cayman Islands as an attractive jurisdiction in line with international developments.

The DPA also serves as a guide to provide assurance to individuals whose personal data is being processed. Indeed, where individuals feel that they are empowered to manage and control their personal data, they are more likely to share personal data with the organisation, to the benefit of both parties.

The Office of the Ombudsman is the Cayman Islands' supervisory authority for data protection. As part of this role, the Ombudsman

- hears, investigates, and rules on complaints;
- monitors, investigates, and reports on compliance by data controllers;
- intervenes and delivers opinions and orders related to processing operations;
- gives orders on rectification, blocking, erasure, or destruction of data;
- imposes temporary and permanent bans on processing;
- makes recommendations for reform both generally and targeted at specific data controllers;
- engages in proceedings where there are violations, and refer violations to the appropriate authorities;
- co-operates with other supervisory authorities;
- publicizes and promotes the requirements of the act and the rights of data subjects; and
- anything else that is conducive or incidental to the Office's functions.

The Office of the Ombudsman's approach to data protection is a practical one. We recognize and respect the fundamental right to privacy. At the same time, we understand that fair and lawful processing of personal data is essential to the modern service economy.

The DPA is modelled on European data protection legislation. Supervisory authorities and court decisions in the European Union will be an important resource for organisations and the Office of the Ombudsman

in interpreting and applying the DPA. However, there are a number of differences between the EU legislation and the DPA which must be taken into account when interpreting the legislation.

The guidance in this document is issued pursuant to sections 34(1) and 41 DPA. It aims to explain how the Office of the Ombudsman will likely interpret certain provisions of the DPA, and is not binding.



Sharon Roulstone
Ombudsman

How to use this guidance

This guidance is addressed to data controllers, i.e. the organisation, business or public authority that controls how the personal data is used. Separate guidance specifically for individuals (data subjects) may be found [here](#).

This guidance aims to explain how the Office of the Ombudsman will likely interpret certain provisions of the DPA, and is not binding.

Typically, each section of the guide includes the following parts:

- *At a glance*: provides a summary of the contents of the section;
- *Checklist*: provides a handhold to help you check your high-level compliance with requirements and best practices under the DPA;
- *In brief*: provides an overview of the individual topics the section addresses;
- *Further guidance*: refers to guidance from other jurisdictions that may be helpful, although it is important that differences between applicable acts are considered; and
- *Relevant provisions*: states the relevant sections of the Data Protection Act.

Please contact us at info@ombudsman.ky if you have any questions or comments.

Acknowledgements

We would like to thank all those who have contributed to this guidance, including Peter Colegate and Peter A. Broadhurst.

Change log

2023-05-05: v1.05 – Removed the threshold for reporting personal data breaches to harmonize guidance with section 16 of the DPA, updated Ombudsman signature on page 3.

2021-09-07: v1.04 – Made additional clarifications on international transfers, amended references to the “Data Protection Law”, the “DPL” and the “Law”, to read: “Data Protection Act (2021 Revision)”, the “DPA” and “Act”, minor adjustments to paragraph spacing, harmonized hyperlinks in footnotes.

2019-01-17: v1.03 – Harmonized terminology; updated sections on: data processors; mixed personal data and subject access requests; international data transfers.

2018-11-07: v1.02 – Added change log, harmonized terminology, minor formatting issues.

Table of Contents

Introduction	2
How to use this guidance	4
Acknowledgements.....	5
Change log.....	6
Key definitions	18
Who does the DPA apply to?	18
What is processing of personal data?	18
What is a data controller?.....	19
When does the DPA apply to me as a data controller?	20
Do you need a local representative?	20
What is a data processor?.....	21
Do service providers always act as data processors?	22
Relevant provisions.....	24
Further guidance.....	24
What information does the DPA apply to?	25
Personal data	25
What is personal data?	26
What identifies a person under the DPA?	26
What is the meaning of 'relates to'?.....	27
What is sensitive personal data?	28
Relevant provisions.....	29
Further guidance.....	29
Data protection principles	30
First Data Protection Principle - Fair and lawful processing	30
Fair processing and the right to be informed	31
Legal processing.....	32
Relevant provisions.....	32
Second data protection principle - Purpose limitation.....	33
What is the purpose limitation principle?	34
Why do you need to specify your purposes?.....	34
How do you specify your purposes?	35
Once you collect personal data for a specified purpose, can you use it for other purposes?	35

What is a 'compatible' purpose?	36
Relevant provisions	37
Third data protection principle - Data minimization	37
What is the data minimization principle?	38
How do you decide what is adequate, relevant and not excessive?	38
When could you be processing too much personal data?	39
When could you be processing inadequate personal data?	40
What about the adequacy and relevance of opinions?	40
Relevant provisions	41
Fourth data protection principle – Data accuracy	42
What is the data accuracy principle?	43
When is personal data 'accurate' or 'inaccurate'?	43
What about records of mistakes?	44
What about accuracy of opinions?	45
Does personal data always have to be up to date?	46
What steps do you need to take to ensure accuracy?	47
What should you do if an individual challenges the accuracy of their personal data?	49
Relevant provisions	49
Fifth data protection principle - Storage limitation	50
What is the storage limitation principle?	51
Why is storage limitation important?	51
Do you need a retention policy?	52
How should you set retention periods?	52
When should you review your retention?	55
What should you do with personal data you no longer need?	55
Do we have to erase personal data from backup systems?	56
How long can you keep personal data for archiving, research or statistical purposes?	56
How does this apply to data sharing from controller to controller?	57
Relevant provisions	57
Sixth data protection principle – Respect for the individual's rights	58
What is the "respect for the individual's rights" principle?	59
What is the right to be informed?	59
What is the right of access?	60

What is the right to rectification?	60
What is the right to stop/restrict processing?	60
What is the right to stop direct marketing?	61
What are the rights in relation to automated decision making?	61
What is the right to complain and seek compensation?	62
Relevant provisions	62
Seventh data protection principle - Security – integrity and confidentiality.....	63
What is the ‘security – integrity and confidentiality principle’?	64
Why should you worry about information security?	65
What do your security measures need to protect?	65
What level of security is required?	66
What organisational measures do you need to consider?	67
What technical measures do you need to consider?	68
What if you operate in a sector that has its own security requirements?	69
What do you do about security when a data processor is involved?	69
Should you use pseudonymization and encryption?	70
What are ‘confidentiality, integrity, availability’ and ‘resilience’?	71
What are the requirements for restoring availability and access to personal data?	71
Are you required to ensure your security measures are effective?	72
What about codes of practice?	73
What about your staff?	73
Relevant provisions	74
Further guidance	74
Eighth data protection principle - International transfers.....	76
Introduction to international transfers.....	76
What is the international transfers principle?	77
What is an adequate level of protection?	77
Are there any derogations from the prohibition on transfers of personal data outside of the EU or other jurisdictions ensuring adequate protection?	78
What terms will the Ombudsman approve as ensuring adequate safeguards?	78
What authorisations will the Ombudsman make?	79
What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?	Error! Bookmark not defined.
What steps should I take when I want to use a service provider not based in the Cayman Islands?	80

My service provider's Data Processing Agreement (DPA) references EU law. Can I use it?	81
Relevant provisions	81
Further guidance	82
Legal basis for processing	83
What is your legal basis for processing?	83
When is processing "necessary"?	84
How do you decide which legal condition applies?	84
When should you decide your legal basis for processing?	87
What happens if you have a new purpose for processing personal data?	87
How should you document the legal basis of your processing?	88
Relevant provisions	89
Further guidance	89
Consent	90
Why is consent important?	92
When is consent appropriate?	92
What is valid consent?	92
How should you obtain, record and manage consent?	93
Relevant provisions	93
Further guidance	94
Contract	95
What does the DPA say?	95
When can I rely on a contract as a condition for processing?	96
When is the legal condition for contracts likely to apply?	96
When is processing 'necessary' for a contract?	97
What else should you consider?	97
Relevant provisions	98
Legal Obligation	99
What does the DPA say?	99
When is the condition for legal obligation likely to apply?	99
When is processing 'necessary' for compliance?	101
What else should you consider?	101
Relevant provisions	101
Vital interests	102

What does the DPA say?	102
What are ‘vital interests’?	103
When is the vital interests condition likely to apply?	103
What else should you consider?	103
Relevant provisions	104
The exercise of public functions	105
What does the DPA say?	105
What is the “public functions” condition for processing?	106
What does “public function” mean?	107
Who can rely on the public function basis?	107
What else should you consider?	107
Relevant provisions	108
Legitimate interests	109
What is the ‘legitimate interests’ basis for processing?	110
When can you rely on legitimate interests?	111
How can you apply legitimate interests in practice?	112
What else do you need to consider?	113
Relevant provisions	114
Sensitive personal data	115
What is “sensitive personal data”?	115
What’s different about sensitive personal data?	116
What are the conditions for processing sensitive personal data?	116
Relevant provisions	118
Further guidance	118
Individual rights	119
The right to be informed	119
What is the right to be informed and why is it important?	121
What privacy information should you provide to individuals?	122
When should you provide privacy information to individuals?	122
What are the exemptions to the right to be informed?	123
How should you draft your privacy information?	124
How should you provide privacy information to individuals?	124
Should you test, review and update your privacy information?	125

The right to be informed in practice	125
Relevant provisions	126
Further guidance	127
The right of access	128
What is the right of access?	129
What is an individual entitled to?	129
Personal data of the individual and mixed personal data	130
How do you recognize a request?	131
Should you provide a specially designed form for individuals to make a subject access request? ..	131
How should you provide the data to individuals?	132
What if the data is already open to access?	132
You have received a request but need to amend the data before sending out the response. Should you send out the “old” version?	132
Do you have to explain the contents of the information you provide to the individual?	133
Can you charge a fee?	134
How long do you have to comply with a subject access request?	134
Can you extend the time for a response?	135
Can you ask an individual for ID?	135
What about requests for large amounts of personal data?	136
What about requests made on behalf of others?	136
What about requests for information about children?	137
What should you do if the data includes information about other people?	138
If we use a processor, does this mean they would have to deal with any subject access requests you receive?	139
Can you refuse to comply with a subject access request?	139
What are the exemptions to the right to access?	140
What should you do if you refuse to comply with a request?	140
Relevant provisions	141
The right to rectification	142
What is the right to rectification?	143
What do you need to do?	143
When is data inaccurate?	144
What should you do about data that records a mistake?	144
What should you do about data that records a disputed opinion?	145

Can you keep processing data while you are considering their accuracy?.....	145
What should you do if you disagree with the request for rectification?.....	145
What are the exemptions to the right to rectification?.....	146
How can you recognize a request for rectification?	146
Can you charge a fee for responding to a request for rectification?.....	146
How long do you have to comply with a request for rectification?	147
Can you ask an individual for ID when they make a request for rectification?	147
Do you have to tell other organisations if you rectify personal data?	147
Relevant provisions	148
The right to stop or restrict processing.....	149
What is the right to stop or restrict processing?	150
When does the right to stop or restrict processing apply?	150
How do you stop or restrict processing?	151
Can you do anything with restricted data?.....	151
Do you have to tell other organisations about ceasing or restricting processing of personal data following a request from an individual?	152
Can you refuse to comply with a request to cease or restrict processing?	152
What are the exemptions to the right to stop or restrict processing?	153
How do you recognize a request to stop or restrict processing?	153
Can you charge a fee for responding to a request to stop or restrict processing?	153
How long do you have to comply with a request to stop or restrict processing?	154
Can you ask an individual for ID?	154
Relevant provisions	154
The right to stop direct marketing	155
What is “direct marketing”?	156
The right to stop direct marketing	156
Do you need to tell individuals about the right to stop direct marketing?	156
Do you always need to erase personal data to comply with a notice to stop direct marketing?	157
Can you refuse to comply with a notice to stop direct marketing?	157
How do you recognize a notice to stop direct marketing?	157
Can you charge a fee for responding to a notice to stop direct marketing?	158
How long do you have to respond to a notice to stop direct marketing?	158
Can you extend the time for a response to a notice to stop direct marketing?.....	158

Can you ask an individual for ID before responding to a notice to stop direct marketing?	158
Relevant provisions	159
Further guidance	159
Rights in relation to automated decision making	160
What is automated individual decision-making?	161
What does the DPA say about automated individual decision-making?	162
What do you need to do under the DPA?	162
Are there circumstances when you do not need to comply with an individual's notice relating to automated processing?	163
What else do you need to consider?	163
Can you charge a fee for responding to a notice to stop automated decision making?	164
How long do you have to respond to a notice relating to automated decision making?	164
Can you extend the time for a response to a notice relating to automated decision making?	164
Can you ask an individual for ID before responding to a notice relating to automated decision making?	164
Relevant provisions	165
Further guidance	165
The right to complain / seek compensation	166
Who can complain to the Ombudsman?	166
What can an individual complain about to the Ombudsman?	166
Will the Ombudsman automatically investigate a complaint?	167
How will the Ombudsman handle offences?	167
Relevant provisions	167
Personal data breaches	168
What is a personal data breach?	169
What breaches do you need to notify the Ombudsman and affected individuals about?	170
What role do processors have?	170
How much time do you have to report a breach?	171
What information must a breach notification to the Ombudsman and the affected individuals contain?	171
What if we don't have all the required information available yet?	171
How do you notify a breach to the Ombudsman?	172
Are there any breaches I do not need tell the affected individuals about?	172
Does the DPA require you to take any other steps in response to a breach?	173

What happens if you fail to notify?	173
Relevant provisions.....	173
Further guidance.....	173
Exemptions	174
National security.....	174
What is exempted?	174
What provisions in the DPA does the exemption relate to?	174
When does the exemption apply?	174
How does the exemption work?	174
Relevant provisions.....	175
Crime, government fees and duties.....	176
What is exempted?	176
What provisions in the DPA does the exemption relate to?	176
When does the exemption apply?	177
Relevant provisions.....	177
Health.....	178
What is exempted?	178
What provisions in the DPA does the exemption relate to?	178
When does the exemption apply?	178
How does this exemption work?	178
Relevant provisions.....	179
Education	180
What is exempted?	180
What provisions in the DPA does the exemption relate to?	180
When does the exemption apply?	180
Relevant provisions.....	181
Social Work	182
What is exempted?	182
What provisions in the DPA does the exemption relate to?	182
When does the exemption apply?	183
What else is there to consider?	183
Relevant provisions.....	183
Monitoring, inspection or regulatory function	184

What is exempted?	184
What provisions in the DPA does the exemption relate to?	184
When does the exemption apply?	184
Relevant provisions.....	185
Journalism, literature or art	186
What is exempted?	186
What provisions in the DPA does the exemption relate to?	186
When does the exemption apply?	186
What else is there to consider?	186
Relevant provisions.....	187
Research, history or statistics	188
What is exempted?	188
What provisions in the DPA does the exemption relate to?	188
When does the exemption apply?	188
What else is there to consider?	189
Relevant provisions.....	189
Information available to public by or under enactments	190
What is exempted?	190
What provisions in the DPA does the exemption relate to?	190
When does the exemption apply?	190
Relevant provisions.....	190
Disclosures required by law or made in connection with legal proceedings	191
What is exempted?	191
What provisions in the DPA does the exemption relate to?	191
When does the exemption apply?	191
Relevant provisions.....	192
Personal, family or household affairs	193
What is exempted?	193
What provisions in the DPA does the exemption relate to?	193
Relevant provisions.....	193
Honours.....	194
What is caught by this exemption?.....	194
What provisions in the DPA does the exemption relate to?	194

Relevant provisions	194
Corporate finance	195
What is exempted?	195
What provisions in the DPA does the exemption relate to?	195
When does the exemption apply?	195
What else is there to consider?	196
Relevant provisions	196
Negotiations.....	197
What is exempted?	197
What provisions in the DPA does the exemption relate to?	197
When does the exemption apply?	197
Relevant provisions	197
Legal professional privilege and trusts	198
What is exempted?	198
What provisions in the DPA does the exemption relate to?	198
Relevant provisions	198
Contracts between data controllers and data processors.....	199
When is a contract needed?	201
What needs to be included in the contract?	201
What responsibilities and liabilities do data processors have in their own right?	202
Relevant provisions	203
Questions or comments?	204

Key definitions

Who does the DPA apply to?

At a glance

- The DPA applies to personal data processed by 'data controllers' and 'data processors'.
- A 'data controller' determines why and how personal data is processed.
- A 'data processor' processes personal data on behalf of a data controller and does not itself determine why personal data should be processed. A data processor may, to a certain extent, decide on how the personal data should be processed.
- A data controller who engages a data processor must ensure that the engagement is based on a written contract which contains certain prescribed assurances regarding the processing of personal data.
- The DPA applies to processing carried out by organisations established within the Cayman Islands, as well as to organisations established outside the Cayman Islands that process personal data within the Cayman Islands.
- The DPA does not apply to processing carried out by individuals purely for personal/household activities.

In brief

- [What is processing of personal data?](#)
- [What is a data controller?](#)
- [When does the DPA apply to me as a data controller?](#)
- [Do you need a local representative?](#)
- [What is a data processor?](#)
- [Do service providers always act as data processors?](#)

What is processing of personal data?

The DPA defines processing very broadly, covering any conceivable use of data. In fact, any activity which affects personal data in any way constitutes processing; mere storage or retention will constitute processing as well.

In relation to personal data, "processing" is:

obtaining, recording or holding data, or carrying out any operation or set of operations on personal data, including -

(a) organising, adapting or altering the personal data;

(b) retrieving, consulting or using the personal data;

(c) disclosing the personal data by transmission, dissemination or otherwise making it available;

or

(d) aligning, combining, blocking, erasing or destroying the personal data;

What is a data controller?

If you exercise control over personal data by making decisions about why and how personal data is handled, you are the data controller.

The DPA defines a “data controller” as:

the person who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed and includes a local representative

As a data controller, you are responsible for applying the requirements of the DPA, applying the data protection principles to the personal data which you process (or which are processed by someone else on your behalf), and cooperating with investigations of the Ombudsman.

As a data controller you are also responsible for ensuring that the data protection principles are complied with in relation to personal data being processed on your behalf (by a data processor).

A data controller can be any legal person, i.e. an individual, corporation, either aggregate or sole, or any club, society, association, public authority or other body, of one or more persons.

Where you, as a data controller, decide together with another organisation about how and why personal data is processed, you will be a joint data controller together with the other organisation. This means that both entities are jointly responsible for complying with their obligations under the DPA. While not explicitly mentioned in the DPA, it is best practice for joint controllers to enter into a joint controllership agreement, which will lay out the parties’ respective responsibilities. It should be noted that the information requirements under the first data protection principle (fair and lawful processing) will mean that the essence of the joint controllership agreement should be communicated to the individual.

When does the DPA apply to me as a data controller?

The DPA applies to you as a data controller if you are:

- established in the Cayman Islands, and the personal data is processed in the context of that establishment; or,
- not established in the Cayman Islands but the data is being processed in the Cayman Islands (otherwise than for transit purposes).

“Established” in the Cayman Islands means:

- you are ordinarily resident in the Islands;
- you are a body incorporated or registered as a foreign company in the Cayman Islands;
- you are a partnership or other unincorporated association formed under Cayman Islands law;
- you maintain an office, branch or agency, or regular practice in the Cayman Islands.

An example of where a data controller is not established in the Cayman Islands but where personal data is being processed in the Cayman Islands other than for transit purposes would be where an overseas entity targets and collects personal data of Cayman residents. The applicability of the DPA will not be triggered simply because a foreign-based service is accessible or available to Cayman residents; there must be an indication that the data controller is seeking out Cayman residents for its service.

Example

An online social network based in a third country solicits Cayman residents as users. The personal data is processed in the Cayman Islands because the personal data of residents is collected locally. The DPA is triggered because the social network actively targets Cayman residents.

Another example of where a data controller is not established in the Cayman Islands but where personal data is being processed in the Cayman Islands is where a data processor within the Cayman Islands processes personal data on behalf of a foreign data controller.

Do you need a local representative?

If you are not established in the Islands but you nevertheless process personal data in the Cayman Islands (otherwise than for transit purposes – see the above section), you must nominate a local representative. You will need to state the local representative in your privacy notice.

Your local representative:

- must be established in the Cayman Islands;
- is, for all purposes within the Islands, the data controller; and,
- bears all obligations of the data controller under the DPA.

What is a data processor?

If you process personal data on behalf of a data controller, and are a separate legal entity from the data controller, you are a data processor.

The DPA defines a “data processor” as:

any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller

As a data processor, you may process personal data which the relevant data controller has entrusted to you only in accordance with the data controller's instructions and the terms of a written agreement (a so-called data processing agreement), which forms the basis of your appointment as a data processor (see below at “[Contracts between data controllers and data processors](#)”).

As a data processor you may not process personal data received from the data controller for your own purposes or in any manner not in accordance with the data controller’s instructions. If you do so, you will become a data controller in your own right and you will bear all obligations of the data controller under the DPA.

Importantly, your role as a data processor or a data controller will depend on the actual decision-making regarding the personal data taking place between the parties, which should be reflected in the legal agreements. The assessment should be from a high-level perspective, taking the whole of the processing activity into consideration.

Example

Within a group of companies, company A may legally have decision-making powers regarding the processing of personal data at company B. Factually, however, all decisions regarding the conditions, manners, and purposes of company B’s processing activities are taken at company B. While the legal arrangement may indicate that company A is the data controller, the actual decision-making taking place means that company B is the data controller.

Do service providers always act as data processors?

Generally, a service provider handles personal data on behalf of and in accordance with instructions given by its client. Nevertheless, a service provider will not be a data processor in all circumstances.

For one, even where a service provider is a true data processor, the service provider may still be a data controller for certain purposes of its own processing activities.

Example

A service provider who uses the client's personal data to perform its own anti-money laundering checks to comply with legal requirements will be acting as a data controller for this purpose. The service provider determines the conditions, manner, and purposes of the processing, obligated by law.

Apart from situations where a data processor is a data controller only for certain purposes, as in the example above, there are situations where a service provider will be a data controller throughout, typically because it enjoys a high degree of independence regarding the processing activity and it cannot be said that the client truly determines the conditions, manner, and purposes of the processing.

As a rule of thumb, a service provider will likely be a data processor where the actual service it provides is focused on the processing of the personal data on behalf of the data controller. In contrast, where the service provider offers a service where the processing of personal data disclosed by the data controller is incidental for the service, without being the core of the service provided, it will likely be a data controller.

This rule of thumb will not always be appropriate, and other factors may need to be considered when assessing whether a service provider is acting as a data processor or a data controller.

Examples

- 1) A catering company is given the names and dietary preferences of guests by the corporate hosts of a commercial dinner party.¹ The core service provided by the catering company is the dinner. The catering company processes the personal data of the guests only incidentally to provide the dinner. The catering company is a data controller and not a data processor.
- 2) A retailer provides the shopping history and details of its female customers to a data analytics company in order to learn which of its customers are pregnant. The core service provided by the data analytics company is the analysis of the personal data. The data analytics company is a data processor.
- 3) Many of the investment funds domiciled in the Cayman Islands do not have a physical presence in the islands and rely on a broad range of service providers to support their business operation.

¹ Data minimization and other data protection principles must be complied with.

- Some service providers (for example providers of registered office services, corporate secretarial services, and fund administration services) engaged by investment funds are, on balance, likely to handle personal data solely for the purposes of providing services to the investment funds, in accordance with a mandate agreed with and provided by the investment funds. Such service providers are likely to act as a data processor.
- Some service providers (for example providers of anti-money laundering compliance services, legal advisors, banks, insurers, etc.) may be exercising a considerable degree of discretion and autonomy in handling personal data in providing their services. Such service providers are likely to act as (joint) data controllers in their own right, even if they are providing a service.
- External directors, when acting in their role as company organ, will fall into none of the above categories. As a company organ, they are deemed to be one and the same as the data controller they direct.

Thus, whether a data controller which engages a service provider should treat the service provider as a data processor will depend very much on the context, and, in particular, the nature of the service provided and the extent to which the service provider exercises autonomy and discretion in deciding what personal data should be handled why and how to provide the services.

Generally, a service provider which performs an outsourced administrative or support function (e.g. back office support, IT support, payroll processing, etc.) is more likely to act as a data processor, while a service provider which provides regulated professional services (e.g. banking, insurance, legal, actuary, accountancy, etc.) is more likely to act as a data controller.

However, such distinction is not definitive and each engagement should be considered on a case by case basis by paying attention to what the service provider is doing with the personal data. There may well be circumstances where a service provider which one might characterize as a processor is in reality acting as a controller (or conversely, a service provider which one might characterize as a data controller is in reality acting as a data processor).

- If a data controller engages a service provider who acts as a data processor, it will need to make sure that the engagement is based on a written contract which conforms to the requirements of the DPA (see [Contracts between data controllers and data processors](#) section below).
- To the extent a service provider which primarily acts as a data processor has a limited need to act as a data controller in its own right, it is best practice to state this in the contract. Additionally, where such service providers are based outside the Cayman Islands, it may also be necessary to put in place additional contractual safeguards to address the cross-border transfer of personal data (see [Eighth data protection principle - International transfers](#) below).
- If a data controller engages a service provider who acts as a data controller, the DPA does not require any specific terms to be agreed with the other data controller. However, if you share personal data with other data controllers, you have a duty to make reasonable efforts to ensure that the receiving data controller will be compliant. The extent of efforts required will depend on the processing activity intended and the type of personal data being disclosed. A data controller might still wish to obtain an assurance that such service providers will comply with the DPA, to the extent applicable. Furthermore, where such service providers are based outside the Cayman

Islands, it may be necessary to put in place additional contractual safeguards to address the cross-border transfer of personal data (see [Eighth data protection principle - International transfers](#) below).

Relevant provisions

Data Protection Act (2021 Revision):²

Section 2:	Definitions
Section 6:	Application of the DPA, duty to nominate a representative
Schedule 2, part 2, para 3:	Processing contract to ensure reliability
Schedule 4, paras 1 and 2	Consent to transfer and contractual provisions
Schedule 4, paras 8-9: Ombudsman	Transfers made on terms approved, or authorised by

Further guidance

Article 29 Working Party:	Opinion 1/2010 on the concepts of “controller” and “processor” ³
---------------------------	---

² https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

³ http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

What information does the DPA apply to?

- **Personal data**

The DPA applies to 'personal data' meaning any information relating to a living individual who can be directly or indirectly identified.

The DPA applies to personal data in any format, including in automated and manual (paper) filing systems.

- **Sensitive personal data**

The DPA refers to 'sensitive personal' data, to which additional protections apply.

Sensitive personal data includes genetic and health data, as well as information on racial or ethnic origins, political opinions, religious or similar beliefs, sex life, the commission or alleged commission of an offence.

Personal data

At a glance

- Understanding whether you are processing personal data is critical to understanding whether the DPA applies to your activities.
- Personal data is information that relates to a living, identified or identifiable individual. If it is possible to identify an individual directly from the information you are processing, then that information will be personal data.
- A number of different factors may identify an individual, including a name or number, as well as online identifiers such as an IP address or cookie identifier, or other factors.
- If you cannot directly identify an individual from the information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it.
- Information which has had identifiers removed or replaced in order to pseudonymize the data may still be personal data for the purposes of DPA if the de-identification measures can be rolled back in any way.

- Information which is truly anonymous is not personal data and is not covered by the DPA.
- Inaccurate or factually incorrect information about a particular individual is still personal data, as it relates to that individual.

In brief

- [What is personal data?](#)
- [What identifies a person under the DPA?](#)
- [What is the meaning of 'relates to'?](#)
- [What is sensitive personal data?](#)

What is personal data?

The DPA applies to the processing of personal data, regardless of its format or storage medium.

Personal data is any information relating to a living, natural person who can be identified.

In other words, data constitutes personal data where the following elements are met:

- (a) the data relates to a living natural person; and
- (c) the identity of the person to whom the data relates is known or identifiable.

Consequently, the following are not subject to the DPA, as they are not deemed to be personal data:

- truly anonymized data;
- information about a deceased person;
- information about companies or public authorities as such. However, information about sole traders, employees, partners, and company directors who are individually identifiable will still constitute personal data.

What identifies a person under the DPA?

Any type of data can be used to identify an individual. A name is perhaps the most common means of identifying someone. However, whether a data or a set of data actually identifies an individual will depend on the overall context of the processing, which must always be taken into consideration when evaluating whether personal data is being processed.

Personal data can either directly or indirectly identify an individual.

The DPA provides a non-exhaustive list of identifiers, including:

- location data;

- online identifiers (which include IP addresses and cookie identifiers);
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
- an expression of opinion about the living individual; and,
- any indication of the intentions of the data controller or another person in respect of the living individual.

If an individual can be identified directly from the information you are processing, it will constitute personal data. This could be a name or a passport number, or a combination of two or more pieces of information from the same data set.

If an individual can be identified indirectly from the information you have, i.e. by combining it with another source of information, the information you have may constitute personal data. That additional information may be information you already hold, or it may be information that you or a third party can reasonably obtain from another source.

As an example, the postal code of an individual will, generally, by itself, not be personal data, as it will not permit a specific individual to be identified. However, taken together with other information, such as an uncommon last name and/or the date of birth and/or gender, the individual may become identifiable.

A mere slight hypothetical possibility that someone could use the data in such a way that identifies the individual will not necessarily be enough to make the individual identifiable in terms of DPA.

When considering whether individuals can be identified, you will have to assess the means that could be used by an interested and sufficiently determined person.

You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

Pseudonymizing data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. Pseudonymization is the de-identification of personal data such that it cannot be attributed to a specific individual without the use of additional information, and where this additional information is kept separate and is subject to technical and organisational measures to prevent any undesired re-identification of the individual. A basic example is the replacing of a direct identifier, such as a name, with a pseudonym, and keeping the list matching the pseudonym with the individual secure and separate.

Inaccurate information may still be personal data if it relates to an identifiable individual.

What is the meaning of 'relates to'?

To be personal data, information must 'relate to', i.e. be about, the identifiable individual. This requirement in effect introduces a further contextual assessment of the data besides the question of identifiability.

To decide whether data relates to an individual, three elements will need to be considered, either of which can independently trigger data as relating to an individual:

- the *content* of the data, i.e. where the data itself is directly about the individual or their activities;
- the *purpose* of the data being processed, i.e. where the data is intended to be used with regards to an individual, such as to evaluate or influence them; and
- the *results* on the individual of the data being processed, i.e. because the processing outcome will impact their rights and interests.

As such, it is important to consider carefully the overall context of the processing activity in order to decide whether the data relates to an individual.

This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant and the data therefore does not relate to them. However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.

An example is where an investigation into a third party's activities was triggered by an individual. The individual submits a subject access request (SAR). The investigation file will not be covered by the SAR; however, the complaint itself and any log of how many investigations have been triggered by the individual will be covered by the SAR.

At times it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

What is sensitive personal data?

The processing of some types of personal data presents a higher risk to that person's rights and interests. The DPA explicitly recognizes certain types of data as being "sensitive personal data"; however, the processing of types of personal data not defined as sensitive under the DPA may, depending on the overall context, also pose a higher risk to a person's rights and interests and warrant an extra level of care.

As a defined term under the DPA, sensitive personal data means personal data consisting of:

- the racial or ethnic origin of the data subject;
- the political opinions of the data subject;
- the data subject's religious beliefs or other beliefs of a similar nature;
- whether the data subject is a member of a trade union;
- genetic data of the data subject;
- the data subject's physical or mental health or condition;
- medical data;
- the data subject's sex life;

- the data subject's commission, or alleged commission, of an offence; or any proceedings for any offence committed, or alleged, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

Processing sensitive personal data requires that at least one condition in each of schedules 2 and 3 applies. See [below](#) for more on sensitive personal data.

Overall, the same considerations apply to sensitive personal data as to personal data in general, in terms of:

- directly or indirectly identifying a living individual; and
- the meaning of "relating to" an individual.

Whether a particular piece of information is sensitive data will depend on a reasonableness test. For example, the unfounded rumor that a head of state is holding someone hostage in their basement will not be held to be sensitive personal data about the alleged commission of an offence.

Relevant provisions

Data Protection Act (2021 Revision):⁴

Section 2:	Definitions
Section 3:	Definition of sensitive personal data
Schedule 2:	Legal bases (conditions) for processing personal data
Schedule 3:	Legal bases (conditions) for processing sensitive personal data

Further guidance

Information Commissioner's Office (UK)(ICO): What is personal data?⁵

⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁵ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/>

Data protection principles

First Data Protection Principle - Fair and lawful processing

At a glance

- You must identify valid grounds under the DPA (known as a 'legal basis') for handling personal data.
- You must ensure that you do not do anything with the data in breach of any other acts.
- You must handle personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about why and how you handle their personal data.

Checklist

Fairness

- ☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- ☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- ☐ We do not deceive or mislead people when we collect their personal data.

Lawfulness

- ☐ We have identified an appropriate lawful basis (or bases) for our processing.
- ☐ If we are processing sensitive personal data, we have identified an applicable condition for processing this type of data.
- ☐ We don't do anything generally unlawful with personal data.

Transparency

- ☐ We are open and honest and we comply with the transparency obligations of the right to be informed.

In brief

- [Fair processing](#)
- [Legal processing](#)

Fair processing and the right to be informed

Processing must always be fair. In general, this means that you should always handle personal data in ways that people would reasonably expect. You should also not handle personal data in any way that would have an unjustifiable adverse effect on them.

Whether processing is fair will depend on the method by which the personal data was obtained, and especially whether the individual was deceived or misled in regard to the purposes for which the data is being processed.

Individuals should be able to make an informed decision. Fairness depends on whether you have made the data subject aware of:

- The identity of the data controller, and;
- The purpose of the data processing.

This information must be communicated to the individual as soon as reasonably practicable. Usually this is done in the form of a [privacy notice](#).

When telling individuals about your processing, always use clear and plain language.

Even if you do not obtain the data directly from the individual, this should not amount to “invisible processing”, and they should be made aware, as would be reasonable under the specific circumstances. In some cases, it will be expected that the individual is directly informed about the processing; in others, a notice on your website may be sufficient.

Fairness will also depend on whether the individual himself has deliberately made the personal data public, and for which purpose. Simply because personal data has been made public does not mean that any processing of that personal data would be fair. The combination of and use of personal data from different sources may produce unexpected effects for the data subject that may be deemed unfair.

Processing is generally considered fair if it is required to be supplied under an enactment, or where a convention or other international instrument imposes a processing obligation.

Legal processing

You need to identify specific legal grounds for processing personal data. Processing is only legal if you meet one of the conditions for processing listed in schedules 2 of the DPA (and additionally, one of the conditions in schedule 3 of the DPA if it is sensitive personal data). If you do not meet these conditions, no lawful basis applies to your processing and your processing will be unlawful and in breach of the first principle ([fair and lawful processing](#)).

Some rights identified in the DPA will not apply depending on the legal basis for processing.

See more on the legal basis for processing [below](#).

See more on the rights of individuals [below](#).

Relevant provisions

Data Protection Act (2021 Revision):⁶

Schedule 1, part 1, paragraph 1:	First data protection principle – Fair and lawful processing
Schedule 1, part 2, paragraphs 1-2:	Interpretation of the first data protection principle
Schedule 2:	Legal bases (conditions) for processing personal data
Schedule 3:	Legal bases (conditions) for processing sensitive personal data

⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Second data protection principle - Purpose limitation

At a glance

- You should be clear about what your purposes for processing are from the start, and you should avoid reusing personal data for different purposes.
- You should record your purposes as part of your processing documentation and specify them in your privacy notice for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you obtain consent, or you have a clear basis in law.

Checklist

- ☐ We have clearly identified our purposes for processing.
- ☐ We have documented those purposes.
- ☐ We include details of our purposes in our privacy information for individuals.
- ☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- ☐ If we plan to use personal data for a new purpose, we check that it is compatible with our original purpose or we get specific consent for the new purpose.

In brief

- [What is the purpose limitation principle?](#)
- [Why do you need to specify your purposes?](#)
- [How do you specify your purposes?](#)
- [Once you collect personal data for a specified purpose, can you use it for other purposes?](#)
- [What is a 'compatible' purpose](#)

What is the purpose limitation principle?

The second data protection principle (in schedule 1 of the DPA) says:

Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

In practice, this means that you must:

- be clear from the outset why you are collecting personal data and what you intend to do with it;
- comply with your transparency obligations to inform individuals about your purposes;
- ensure that if you plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

As well, it is best practice to:

- document the purposes for processing upfront.

Why do you need to specify your purposes?

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes from the outset and refraining from repurposing helps you to be accountable for your processing, and helps you avoid ‘scope creep’. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over their personal data where appropriate. It is fundamental to building public trust in how you use personal data.

There are clear links with other principles – in particular, the [fair and lawful processing principle](#). Being clear about why you are processing personal data will help you to ensure your processing is fair, lawful, and transparent. Using data for unfair, unlawful or ‘invisible’ reasons is likely to be a breach of both principles.

Specifying your purposes is [required](#) in terms of being accountable for your processing.

How do you specify your purposes?

If you comply with your fairness and transparency obligations, you are likely to comply with the requirement to specify your purposes without doing anything more:

- You need to specify your purpose or purposes for processing personal data in your privacy notice for individuals.
- It is best practice to keep detailed documentation on your data processing activities, including all your purposes. This is not a legal requirement under DPA, however, it is vital to have good documentation to be able to respond to subject access requests, cooperate with investigations by the Ombudsman, and inform individuals what you do with their data.

Remember that whatever you document, and whatever you tell people, this cannot make fundamentally unfair processing fair and lawful.

If you have not provided privacy information (see below on ['The Right to be Informed'](#)) because you are only using personal data for an obvious purpose that individuals already know about, e.g. processing employees' data, the "specified purpose" should be taken to be the obvious purpose.

You should regularly review your processing, documentation and privacy information to check that your purposes have not evolved over time beyond those you originally specified ('function creep').

Once you collect personal data for a specified purpose, can you use it for other purposes?

The DPA does not ban this altogether, but there are restrictions. In essence, if your purposes change over time or you want to use data for a new purpose which you did not originally anticipate, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

If your new purpose is compatible, you don't need a new lawful basis for the further processing. However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful.⁷

⁷ See: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

You also need to make sure that you update your [privacy notice](#) to ensure that your processing is still transparent.

What is a 'compatible' purpose?

The DPA specifically says that the following purposes can be considered to be compatible purposes:

- research purposes (in this context 'research' is understood to be scientific research);
- historical research purposes; and
- statistical purposes.⁸

Other purposes can still be compatible, depending on the context. When deciding whether a new purpose is compatible with your original purpose it is best practice to take into account:

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – e.g. is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards – e.g. encryption or pseudonymization.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose data for the new purpose.

Example

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

There are clear links here with the [fair and lawful processing](#) principle. In practice, if your intended processing is fair, you are unlikely to breach the [purpose limitation principle](#) on the basis of incompatibility.

⁸ DPA s.23(4)

Relevant provisions

Data Protection Act (2021 Revision):⁹

Schedule 1, Part 1, paragraph 2: Second data protection principle – Purpose limitation

Section 23(4): Compatible purposes - research, history and statistics

Third data protection principle - Data minimization

At a glance

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Checklist

- ☐ We only collect personal data we actually need for our specified purposes.
- ☐ We have sufficient personal data to properly fulfil those purposes.
- ☐ We periodically review the data we hold, and delete anything we don't need.

In brief

- [What is the data minimization principle?](#)
- [How do you decide what is adequate, relevant and not excessive?](#)
- [When could you be processing too much personal data?](#)
- [When could you be processing inadequate personal data?](#)
- [What about the adequacy and relevance of opinions?](#)

⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

What is the data minimization principle?

The third data protection principle says:

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

You should identify the minimum amount of personal data you need to fulfil your purpose. You should process that much information, but no more.

This is the first of three principles about data standards, along with [data accuracy](#) and [storage limitation](#).

When asked by the Ombudsman, you should be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that if your processing is excessive, you are less likely to benefit from the legal exemptions to the rights individuals have under Section 10 of the DPA, which allows individuals to require you to [stop processing](#) their personal data.

How do you decide what is adequate, relevant and not excessive?

The DPA does not define these terms. Clearly, though, this will depend on your specified purpose for collecting and using the personal data. It may also differ from one individual to another.

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it.

For sensitive personal data, it is particularly important to make sure you collect and retain only the minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should in particular consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need. This is closely linked with the [storage limitation principle](#).

When could you be processing too much personal data?

You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details.

Example

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search, if necessary. It may be appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

If you need to process particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.

Example

A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

Example

An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.

If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach of the third data protection

principle dealing with [data minimization](#). Individuals will also have the right to demand that [processing cease](#).

When could you be processing inadequate personal data?

If the processing you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should avoid processing personal data if it is insufficient for its intended purpose. For example, a data controller should not make a decision which affects a data subject if the personal data in respect of that data subject is or may be incomplete.

In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.

Example

A group of individuals set up a club. At the outset the club has only a handful of members, who all know each other, and the club's activities are administered using only basic information about the members' names and email addresses. The club proves to be very popular and its membership grows rapidly. It becomes necessary to collect additional information about members so that the club can identify them properly, and so that it can keep track of their membership status, subscription payments etc.

Data may also be inadequate if you are making decisions about someone based on an incomplete understanding of the facts. In particular, if an individual asks you to supplement incomplete data under their [right to rectification](#), this could indicate that the data might be inadequate for your purpose.

Obviously it makes no business sense to have inadequate personal data – but you must be careful not to go too far the other way and collect more than you need.

What about the adequacy and relevance of opinions?

The definition of personal data includes the expression of an opinion about a living individual and any indication of intentions in respect of the living individual.

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarizes more detailed records held elsewhere, you should make this clear.

Example

A GP's record may hold only a letter from a consultant and it will be the hospital file that contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable detailed records to be traced.

For more information about the accuracy of opinions, see our guidance on the [data accuracy principle](#).

Relevant provisions

Data Protection Act (2021 Revision):¹⁰

Schedule 1, part 1, paragraph 3:	Third data protection principle – Data minimization
Schedule 1, part 1, paragraph 4:	Fourth data protection principle – Data accuracy

¹⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Fourth data protection principle – Data accuracy

At a glance

- You should take all reasonable steps to ensure the personal data you handle is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges individuals make regarding the accuracy of their personal data.

Checklist

- ☐ We ensure the accuracy of any personal data we create.
- ☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- ☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- ☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.
- ☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- ☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- ☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

In brief

- [What is the data accuracy principle?](#)
- [When is personal data 'accurate' or 'inaccurate'?](#)
- [What about records of mistakes?](#)
- [What about accuracy of opinions?](#)

- [Does personal data always have to be up to date?](#)
- [What steps do you need to take to ensure accuracy?](#)
- [What should you do if an individual challenges the accuracy of their personal data?](#)

What is the data accuracy principle?

The fourth data protection principle says:

Personal data shall be accurate and, where necessary, kept up to date.

This is the second of three principles about data standards, along with [data minimization](#) and [retention limitation](#).

There are clear links to section 14 of the DPA, which gives individuals the right to have inaccurate personal data [corrected](#).

In practice, this means that you must:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source and status of personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

When is personal data 'accurate' or 'inaccurate'?

The DPA defines the word "inaccurate" as follows:

"inaccurate", in relation to personal data, includes data that are misleading, incomplete or out of date.

Whether information is accurate or not will be a matter of fact, and will usually be obvious.

You must always be clear about what you intend the record of the personal data to show. What you use it for may affect whether it is accurate or not. For example, just because personal data has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record.

Example

If an individual moves house from Bodden Town to West Bay a record saying that they currently live in Bodden Town will obviously be inaccurate. However a record saying that the individual once lived in Bodden Town remains accurate, even though they no longer live there.

Also bear in mind that section 14 of the DPA, you could be ordered to correct inaccuracy or incompleteness in personal data (or to delete inaccurate or incomplete personal data) you hold, if a complaint made by the relevant individual is upheld.

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded.

However, you may legitimately need your records to accurately reflect the order of events – in this example, that a charge was imposed, but later cancelled or refunded. Keeping a record of the mistake and its correction might also be in the individual's best interests.

Example

A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.

It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

If you do not act accordingly, and the individual makes a complaint to the Ombudsman, the latter may issue an order that the personal data be supplemented by a statement of facts. In reaching a decision the Ombudsman will consider the purposes for which the data is being processed. The statement may indicate the individual's view that the data is inaccurate.

When the Ombudsman is satisfied that personal data is inaccurate, she may require that third parties to whom the data has been disclosed be notified that the data has been [rectified](#), [blocked](#), [erased or destroyed](#), except if it is not reasonably practical to do so.

Example

An individual finds that, because of an error, their account with their existing energy supplier has been closed and an account opened with a new supplier. Understandably aggrieved, they believe the original account should be reinstated and no record kept of the unauthorised transfer. Although this reaction is understandable, if their existing supplier did close their account, and another supplier opened a new account, then records reflecting what actually happened will be accurate. In such cases it makes sense to ensure that the record clearly shows that an error occurred.

What about accuracy of opinions?

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

Nonetheless, where appropriate the Ombudsman may order the rectification, blockage, erasure or destruction of expressions of opinion based on inaccurate personal data. [s.14(1)]

Example

An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (which is an informed opinion) may prove to be incorrect after more extensive examination or further tests. However, if the patient's records reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect that doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later, and in data protection terms is required in order to comply with the 'adequacy' element of the data minimization principle.

If an individual challenges the accuracy of an opinion, it is good practice to add a note recording the challenge and the reasons behind it.

How much weight is actually placed on an opinion is likely to depend on the experience and reliability of the person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. However, this is not really an issue of accuracy. Instead, you need to consider whether the personal data is “adequate” for your purposes, in line with the [data minimization](#) principle.

Note that some records which may appear to be opinions do not contain an opinion at all. For example, many financial institutions use credit scores to help them decide whether to provide credit. A credit score is a number that summarizes the historical credit information on a credit report and provides a numerical predictor of the risk involved in granting an individual credit. Credit scores are based on a statistical analysis of individuals’ personal data, rather than on a subjective opinion about their creditworthiness. However, you must ensure the accuracy (and adequacy) of the underlying data.

Does personal data always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers’ changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information. Indeed, in some cases it may be necessary to preserve inaccurate or incomplete personal data, for example as part of an audit or complaints handling record.

Example

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

You do not need to update personal data if doing so would defeat the purpose of the processing. For example, if you hold personal data only for [statistical, historical or other \(scientific\) research](#) reasons, updating the data might defeat that purpose.

In some cases it is reasonable to rely on the individual to tell you when their personal data has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this.

Example

An organisation keeps addresses and contact details of previous customers for marketing purposes. It does not have to use data matching or tracing services to ensure its records are up to date – and it may actually be difficult to show that the processing involved in data matching or tracing for these purposes is fair, lawful and transparent.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message ‘not at this address’ marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should delete the address from its database, unless there is a valid reason for keeping the inaccurate personal data.

Depending on the nature of the processing activity, and where there is a need to prevent inaccurate or outdated data from influencing future processing outcomes, it may also be warranted to keep a hash of the inaccurate personal data instead of the personal data itself in clear form. This will reflect the third (data minimization) and fifth (storage limitation) data protection principles of the DPA.

What steps do you need to take to ensure accuracy?

Where you use your own resources to compile personal data about an individual, you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. If, for example, you give an employee a pay increase on the basis of an annual increment and a performance bonus, then there is no excuse for getting the new salary figure wrong in your payroll records.

It may be impractical to check the accuracy of personal data someone else provides. In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

What is a 'reasonable step' will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate. For example, employers may need to check the precise details of job applicants' education, qualifications and work experience if it is essential for that particular role, when they would need to obtain authoritative verification.

Example

An organisation recruiting a driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in his work history that he worked as a Father Christmas in a department store 20 years ago does not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it is usually reasonable to assume that they have given you accurate information. However, in some circumstances you need to double-check – for example if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.

Example

A business that is closing down recommends a member of staff to another organisation. Assuming the two employers know each other, it may be reasonable for the organisation to which the recommendation is made to accept assurances about the individual's work experience at face value. However, if a particular skill or qualification is needed for the new job role, the organisation needs to make appropriate checks.

Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible.

What should you do if an individual challenges the accuracy of their personal data?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it unless it is necessary to preserve the information in its inaccurate state (e.g. as part of an audit or complaints handling record).

Individuals may complain to the Ombudsman who may order that inaccurate data be [rectified](#), [blocked](#), [erased or destroyed](#).

You should rectify, block, erase or destroy inaccurate personal data without delay, in particular when ordered to do so by the Ombudsman following a complaint by an individual. This may include any expression of opinion that appears to the Ombudsman to be based on the inaccurate data.

Also remember that individuals are entitled to require that you [cease processing](#) their personal data, in general, for a specified purpose or in a specified manner.

It may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data it is therefore good practice to consider this request.

Relevant provisions

Data Protection Act (2021 Revision):¹¹

Schedule 1, part 1, paragraph 4: Fourth data protection principle – Data accuracy

Section 14: Rectification, blocking, erasure or destruction

¹¹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Fifth data protection principle - Storage limitation

At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymize it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, [scientific or historical research, or statistical purposes](#).

Checklist

- ☐ We know what personal data we hold and why we need it.
- ☐ We carefully consider and can justify how long we keep personal data.
- ☐ We have a policy with standard retention periods where possible.
- ☐ We regularly review our information and erase or anonymize personal data when we no longer need it.
- ☐ We have appropriate processes in place to comply with individuals' requests for erasure under the [right to stop or restrict processing](#).
- ☐ We clearly identify any personal data that we need to keep for public interest archiving, [scientific or historical research, or statistical purposes](#).

In brief

- [What is the storage limitation principle?](#)
- [Why is storage limitation important?](#)
- [Do you need a retention policy?](#)
- [How should you set retention periods?](#)
- [When should you review your retention?](#)
- [What should you do with personal data you no longer need?](#)
- [How long can you keep personal data for archiving, research or statistical purposes?](#)
- [How does this apply to data sharing?](#)

What is the storage limitation principle?

The fifth data protection principle says:

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

So, even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it.

There are close links here with the third ([data minimization](#)) and fourth ([data accuracy](#)) data protection principles.

The DPA does not set specific time limits for different types of data. This is up to you, and will depend on how long you need the data for your specified purposes, or how long you are required to maintain the data to comply with legal or regulatory requirements.

Why is storage limitation important?

Ensuring that you erase or anonymize personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimization and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than you need, and there may be unnecessary costs associated with storage and security.

Remember that you must also respond to [subject access requests](#) for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

Do you need a retention policy?

Retention policies or retention schedules list the types of record or information you hold, what you use them for, and how long you intend to keep them. They help you establish and document standard retention periods for different categories of personal data.¹²

A retention schedule may form part of a broader 'information asset register' (IAR), or your personal data documentation.

It is best practice to establish and document standard retention periods for different categories of information you hold wherever possible. It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate (for instance, in certain circumstance when an individual withdraws their consent or requires that you cease processing their data). If you are not actually using a record, you should reconsider whether you need to retain it.

If you are a small organisation, do not keep large amounts of data or undertake only occasional low-risk processing, you may not need a documented retention policy.

However, if you don't have a retention policy (or if it doesn't cover all of the personal data you hold), you must still regularly review the data you hold, and delete or anonymize anything you no longer need.

How should you set retention periods?

The DPA does not dictate how long you should keep personal data. It is up to you to justify this, based on your purposes for processing. You are in the best position to judge how long you need it. There may be other applicable statutory record retention requirements.

¹² For examples applicable in the Cayman Islands Government, see: <http://www.cina.gov.ky/>

You must also be able to justify why you need to keep personal data in a form that permits identification of individuals. If you do not need to identify individuals, you should anonymize the data so that identification is no longer possible.

- You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies, but you should not keep data indefinitely 'just in case', or if there is only a small possibility that you will use it.

Example

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons for a set period.

Example

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – the agency should remove it from their systems unless there are good reasons for keeping it. Such reasons could include if the agency has also been asked to collect the debt, or because the agency is authorised to use the information to trace debtors on behalf of other creditors.

Example

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends.

Example

A business may need to keep some personal data about a previous customer so that they can deal with any complaints the customer might make about the services they provided.

You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.

Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

Example

An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or beneficiary details.

Example

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for [direct marketing](#). It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.
- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for audit purposes, or information on aspects of health and safety. For example, public authorities have to follow the National Archive and Public Records Act (2015 Revision) in retaining/disposing records, while entities which are regulated by the Cayman Islands Monetary Authority (“CIMA”), or which otherwise carry on “relevant financial business” for the purposes of compliance with anti-money laundering acts are required to keep data for specified periods. If you keep personal data to comply with an express legal requirement like these, you will not be considered to have kept the information for longer than necessary.
- You should consider any relevant industry standards or guidelines. For example, credit reference agencies may be permitted to keep consumer credit data for six years. Industry guidelines are a good starting point for standard retention periods and are likely to take a considered approach.

However, they do not guarantee compliance. You must still be able to explain why those periods are justified, and keep them under review.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and meet [legal conditions for processing](#).

When should you review your retention?

You should review whether you still need personal data at the end of any standard retention period, and erase or anonymize it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful if you hold many records of the same type.

It is also good practice to review your retention of personal data at regular intervals before this, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

If you don't have a set retention period for the personal data, you must regularly review whether you still need it.

However, there is no firm rule about how regular these reviews must be. Your resources may be a relevant factor here, along with the privacy risk to individuals. The important thing to remember is that you must be able to justify your retention and how often you review it.

You must also review whether you still need personal data if the individual asks you to. Individuals have the absolute right to erasure of personal data that you no longer need for your specified purposes.

What should you do with personal data you no longer need?

You can either erase (delete) it, or anonymize it.

You need to remember that there is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still processing personal data. You should only store it offline (rather than delete it) if you can still justify holding it. You must be prepared to respond to [subject access requests](#) for personal data stored offline, and you must still comply with all the other principles and rights.

The word 'deletion' can mean different things in relation to electronic data, and it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information, subject to reasonability.

Alternatively, you can anonymize the data so that it is no longer “in a form which permits identification of data subjects”.

Personal data that has been pseudonymized – e.g. key-coded – will usually still permit identification. Pseudonymization can be a useful tool for compliance with other principles such as [data minimization](#) and [security – integrity and confidentiality](#), but the storage limitation principle still applies.

Do we have to erase personal data from backup systems?

If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in regard to backups), and the technical mechanisms that are available to you.

You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It may be that the erasure request can be instantly fulfilled in your live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

The key issue is to put the backup data ‘beyond use’, even if it cannot be immediately overwritten. In any event, you must ensure, through technical and organisational measures, that you do not use the data within the backup for any other purpose, i.e. that the backup is simply held on your systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will depend on the specific context.

How long can you keep personal data for archiving, research or statistical purposes?

Personal data processed for [historical, statistical, or scientific](#) purposes in compliance with the relevant conditions are exempt from the [fifth data protection principle](#) (storage limitation) to the extent to which compliance would be likely to prejudice those purposes.

You can keep personal data indefinitely if you are holding it only for those purposes. The general rule that you cannot hold personal data indefinitely ‘just in case’ does not apply if you are keeping it for these historical, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. For example, pseudonymization may be appropriate in some cases.

This must be your only purpose. If you justify indefinite retention on this basis, you cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. This does not

prevent other organisations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the data protection principles.

How does this apply to data sharing from controller to controller?

The DPA does not explicitly address this question. However, if you share personal data with other controllers, you have a duty to make reasonable efforts to ensure that the receiving controller will be compliant. The extent of efforts required will depend on the processing activity intended and the type of personal data being disclosed. Apart from that, it bears keeping in mind that you will need to have a legal basis for the disclosure of the personal data (as it is a processing itself), and the other controller will need to have a legal basis for their own processing.

As such, it is best practice to agree upfront on the handling of the shared data, especially for when you no longer need to share the data. In some cases, it may be best to return the shared data to the organisation that supplied it without keeping a copy. In other cases, each of the organisations involved should delete their copies of the personal data.

Example

Personal data about the customers of Company A is shared with Company B, compliant with all data protection principles. Company B is negotiating to buy Company A's business. The companies arrange for Company B to keep the information confidential, and use it only in connection with the proposed transaction. The sale does not go ahead and Company B returns the customer information to Company A without keeping a copy.

The organisations involved in an information-sharing initiative may each need to set their own retention periods, because some may have good reasons to retain personal data for longer than others. However, if each organisation only holds the data for the purposes of the data-sharing initiative and it is no longer needed for that initiative, then all organisations with copies of the information should delete it.

Relevant provisions

Data Protection Act (2021 Revision):¹³

Schedule 1, part 1, paragraph 5: Fifth data protection principle – Storage limitation

¹³ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Sixth data protection principle – Respect for the individual’s rights

At a glance

- The DPA grants certain rights to individuals in relation to their personal data and how it is processed.
- You must process all personal data in accordance with the rights of individuals.
- You should plan ahead in order to prepare for responding to each of the likely requests and notices you may receive and meet the statutory timelines.
- In order to respond in a timely fashion to requests and notices from individuals you should have certain information readily available. This includes what personal data you have, where you keep it, what the legal basis is of all your processing, where you obtained it, who you share it with, how long you keep it, and how you intend to delete it once required.

Checklist

- ☐ We respect the [right to be informed](#) by notifying each individual about our identity and the purpose(s) of processing as soon as possible.
- ☐ We know what personal data we have on each individual, and are ready to respond to [requests for access](#) within the 30-day timeline.
- ☐ We have procedures in place to respond to individual’s requests to have inaccurate data [rectified and execute on them where substantiated](#).
- ☐ We are ready to respond to notices from individuals who require that we [stop processing](#) their data in whole or in relation to certain purposes or in certain manners.
- ☐ We are ready to [stop direct marketing](#) in respect of individuals who notify us.
- ☐ We notify individuals when we take decisions that affect them based solely on [automatic means](#), and we are ready to reconsider it on a different basis.

In brief

- [What is the “respect for the individual’s rights” principle?](#)
- [What is the right to be informed?](#)
- [What is the right of access?](#)
- [What is the right to rectification?](#)
- [What is the right in relation to automated decision making?](#)
- [What is the right to complain and seek compensation?](#)

What is the “respect for the individual’s rights” principle?

The sixth data protection principle says:

Personal data shall be processed in accordance with the rights of data subjects under this Act.

This principle underscores the importance of all the rights of individuals under the DPA:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to stop/restrict processing;
- The right to stop direct marketing;
- The right in relation to automated decision making; and
- The right to complain and seek compensation.

What is the right to be informed?

The right to be informed follows from the [first data protection principle](#) (fair and lawful processing).

Processing will only be fair if personal data is handled in ways that people would reasonably expect. This includes being told what the identity of the data controller and the purpose(s) for processing are. This is done in the privacy notice which is provided to the individual as soon as practicable, which is usually when the data is being gathered.

Depending on the nature of the processing activity, although not explicitly required by the DPA, fairness may also require you to provide information on who you will share it with, any international data transfers, how long it will be kept for, and the technical and organisational measures taken to comply with the [seventh data protection principle](#) (security – integrity and confidentiality).

You will find more on the right to be informed [here](#).

What is the right of access?

Individuals have the [right to access](#) their own personal data and receive information about its use. There are some exemptions to this right.

You have one month to respond to a subject access request.

There is no fee, except in exceptional circumstances further explained below.

You will find more on the right of access [here](#).

What is the right to rectification?

Individuals have a right to have inaccurate personal data rectified, blocked, erased or destroyed.

The right to rectification operates slightly different from other individual rights. The DPA does not expressly grant individuals the right to ask you to correct inaccuracies in their personal data, but individuals have a right to complain about inaccurate personal data and where such complaint is upheld, you can be compelled to correct the inaccuracy or delete the inaccurate personal data.

Notwithstanding this, the Ombudsman would expect organisations to deal with reasonable requests for rectification directly as a matter of good practice, instead of waiting for a formal complaint to be made and upheld.

Having accurate information is to the benefit of the data controller as well as the individual.

You will find more on the right to rectification [here](#).

What is the right to stop/restrict processing?

The DPA introduces a right for individuals to demand that processing cease. However, this right is not absolute.

An individual may require that you:

- cease processing their personal data;
- not begin processing their personal data;

- cease processing their personal data for a specified purpose; or
- cease processing their personal data in a specified manner.

You must comply with this request, unless the processing is done to meet the conditions of a contract (or is undertaken as a step towards engaging in a contract), when it is done under a legal obligation, or in order to protect the vital interest of the individual.

Certain exemptions also apply to the right to stop processing.

You will find more on the right to stop/restrict processing [here](#).

What is the right to stop direct marketing?

The DPA introduces an absolute right for individuals to demand that direct marketing targeting the individual cease or not begin.

Direct marketing is defined as:

the communication, by whatever means, of any advertising, marketing, promotional or similar material, that is directed to particular individuals.

You will find more on the right to stop direct marketing [here](#).

What are the rights in relation to automated decision making?

Where a decision is made solely by automated means (without human involvement), an individual has the right to require that it be reconsidered on a different basis.

You need to notify individuals when such decisions are made solely on an automated basis, and respond to written notifications from individuals within legal timelines outlining the steps taken to comply.

This right relates to automated decisions which affect the individual, for example for the purpose of evaluating the individual's performance at work, creditworthiness, reliability, conduct or any other matters relating to the individual.

You do not need to comply with an individual's notice if the decision is taken:

- for the purpose of considering whether to enter into a contract with the individual; or
- in the course of performing such a contract,

and:

- the decision is to grant a request of the individual; or
- the individual's interests are safeguarded by allowing them to make representations.

You will find more on the rights in relation to automated decision making [here](#).

What is the right to complain and seek compensation?

An individual has the right to complain to the Ombudsman about any perceived violation of the DPA, and to seek compensation for damages in the courts.

You will find more on the right to complain and seek compensation [here](#).

Relevant provisions

Data Protection Act (2021 Revision):¹⁴

Schedule 1, part 1, paragraph 6:	Sixth data protection principle – respect for the individual’s rights
Schedule 1, part 2, paragraph 2:	Specified information at the relevant time
Sections 8-9:	Fundamental right of access to personal data
Section 14:	Rectification, blocking, erasure or destruction
Section 10:	Right to stop processing
Section 11:	Right to stop processing for direct marketing
Sections 8(3) and 12:	Rights in relation to automated decision making

¹⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Seventh data protection principle - Security – integrity and confidentiality

At a glance

- A key principle of the DPA is that you process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security – integrity and confidentiality principle’.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- The security requirements also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymization and encryption.
- Your measures should ensure the ‘confidentiality, integrity and availability’ of the personal data you process.
- You should ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

Checklist

- ☐ We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.
- ☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- ☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- ☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- ☐ We use encryption and/or pseudonymization where it is appropriate to do so.
- ☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.

- ☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- ☐ We conduct regular testing and reviews of our measures to ensure they remain effective and up to date, and act on the results of those tests where they highlight areas for improvement.
- ☐ We ensure that any data processor we use also implements appropriate technical and organisational security measures.

In brief

- [What is the 'security – integrity and confidentiality principle'?](#)
- [Why should you worry about information security?](#)
- [What do your security measures need to protect?](#)
- [What level of security is required?](#)
- [What organisational measures do you need to consider?](#)
- [What technical measures do you need to consider?](#)
- [What if you operate in a sector that has its own security requirements?](#)
- [What do you do when a data processor is involved?](#)
- [Should you use pseudonymization and encryption?](#)
- [What are 'confidentiality, integrity, availability' and 'resilience'?](#)
- [What are the requirements for restoring availability and access to personal data?](#)
- [Are you required to ensure our security measures are effective?](#)
- [What about codes of conduct?](#)
- [What about your staff?](#)

What is the 'security – integrity and confidentiality principle'?

The seventh data protection principle says:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

There are different aspects to this principle, including:

- Organisational measures e.g. staff training and policy development;
- Technical measures e.g. physical protection of data, pseudonymization, encryption;
- Securing ongoing availability, integrity and accessibility, e.g. by ensuring backups.

Why should you worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses or informers put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognize that individuals are also entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the DPA and other acts you may be subject to.

The Ombudsman will consider the technical and organisational measures you had in place when considering an administrative fine.

What do your security measures need to protect?

The security – integrity and confidentiality principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just IT security. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and

- the data remains accessible and usable to those who have a legitimate need to access and use it, i.e. if personal data is accidentally lost, altered or destroyed, you should be able to recover it

These measures should ensure 'confidentiality, integrity and availability'. Under the DPA they constitute best practice.

What level of security is required?

The DPA does not define the security measures that you should have in place. The Act requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects the DPA's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation and the individuals whose data you process.

For a small business this may mean little more than ensuring that the office and filing cabinet are locked and staff are aware of the personal and confidential nature of the information that is held. In larger organisations, or businesses that process personal data with higher levels of risk (e.g. health data), this may involve more complex organisational and technical measures.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

We cannot provide a complete guide to all aspects of security in all circumstances for all organisations, but this guidance is intended to identify the main points for you to consider.

What organisational measures do you need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you may need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively.

Example

The Head of a medium-sized organisation asks the Resources Manager to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Clear accountability for security will ensure that you do not overlook these issues, and that your overall security posture does not become flawed over time.

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on the size of your organisation, the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security – integrity and confidentiality principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (e.g. how to decommission and dispose of any IT equipment that may contain personal data);
- access to premises or equipment given to anyone outside your organisation (e.g. for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold in case of an emergency; and
- periodic monitoring to ensure that your security measures remain appropriate and up to date.

What technical measures do you need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. While these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the inappropriate disposal of old computers, or hard-copy (paper) records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, particularly those which process personal data;
- data security – the security of the data you hold within your systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
- online security – e.g. the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it may also be that you do not need a great deal of time and resources to secure your systems and the personal data they process.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;
- you should take into account the state of technological development, but also the costs of implementation;

- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

What if you operate in a sector that has its own security requirements?

Some industries have specific security requirements or require you to adhere to certain frameworks or standards. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators. If you operate in these sectors, you need to be aware of their requirements, particularly if specific technical measures are specified.

Although following these requirements will not necessarily equate to compliance with the DPA's security – integrity and confidentiality principle, the Ombudsman will nevertheless consider these carefully in any considerations of regulatory enforcement action.

Example

If you are processing payment card data, you may be obliged to comply with the [Payment Card Industry Data Security Standard](#). The PCI-DSS outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the DPA's security – integrity and confidentiality principle, if you process card data and suffer a personal data breach, the Ombudsman will consider the extent to which you have put in place measures that PCI-DSS requires, particularly if the breach related to a lack of a particular control or process mandated by the standard.

What do you do about security when a data processor is involved?

If an organisation processes personal data on your behalf, then it is a data processor under the DPA. A common example in the Cayman Islands financial services context will be where a mutual fund engages an administrator. Your own employees are not considered data processors under the DPA.

This can cause security problems – as a data controller you are responsible for ensuring compliance with the DPA and this includes what the data processor does with the data. However, in addition to this, the DPA's security requirements also apply to any data processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its technical and organisational security measures. Conducting appropriate due diligence as part of supply chain management is good practice, and may also be required by e.g. CIMA guidance;
- you must have a written contract (a “data processing agreement”) that stipulates that the data processor acts only on instructions from yourself (the data controller), and that the data processor must undertake the same security measures that you would have to take if you were doing the processing yourself; and
- depending on the nature of the processing and the risk posed by the data processor, you may consider including in the data processing agreement provisions that require the data processor to provide you with appropriate information and assistance to help you comply with the DPA (e.g. in relation to any audit or investigation the Ombudsman may perform in relation to your organisation). This may also include, where appropriate, allowing you to audit and inspect the data processor to make sure they are in compliance with the contract and their obligations under the Act.

At the same time, your data processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a data processor that has these resources can assist you in making sure personal data is processed securely, provided that your [contractual arrangements](#) are appropriate.

Should you use pseudonymization and encryption?

Pseudonymization and encryption are two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. Whether you do will depend on the nature, scope, context, and purposes of your processing, and the risks posed to individuals.

However, there are a wide range of solutions that allow you to implement both without great cost or difficulty. For example, for a number of years encryption has been widely used as an appropriate technical protection measure given its widespread availability and relatively low cost of implementation. The DPA does not change this. If you are storing personal data, or transmitting it over the internet, we recommend that you use encryption and have a suitable policy in place, taking account of the residual risks involved.

When considering what to put in place, you should undertake a risk analysis and document your findings.

What are 'confidentiality, integrity, availability' and 'resilience'?

Collectively known as the 'CIA triad', confidentiality, integrity, and availability are the three key elements of information security. If any of the three elements is compromised there can be serious consequences, both for you as a data controller, and for the individuals whose personal data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

The CIA triad has existed for a number of years and its concepts are well-known to security professionals.

You are also required to have the ability to ensure the 'resilience' of your processing systems and services. Resilience refers to:

- whether your systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
- your ability to restore them to an effective state.

This refers to things like business continuity plans disaster recovery, and the ability of your IT systems to resist or withstand adverse incidents. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

What are the requirements for restoring availability and access to personal data?

Having appropriate organisational and technological security measures includes having the ability to restore the availability of, and access to, personal data in the event of a physical or technical incident in a 'timely manner'.

The DPA does not provide details on this, and the applicability of this rule will depend on the context and in particular:

- the nature of your organisation and processing purposes, including the risk for individuals if the personal data you process is unavailable for a period of time;
- the type of systems used.

The key point is that you should take these elements into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.

Example

An organisation takes regular backups of its systems and the personal data held within them. It follows the well-known '3-2-1' backup strategy: three copies, with two stored on different devices and one stored off-site.

The organisation is targeted by a ransomware attack that results in the data being encrypted. This means that it is no longer able to access the personal data it holds.

Depending on the nature of the organisation and the data it processes, this lack of availability can have significant consequences for individuals and would constitute a personal data breach under the DPA.

The ransomware has spread throughout the organisation's systems, meaning that two of the backups are also unavailable. However, the third backup, being stored off-site, allows the organisation to restore its systems in a timely manner. There may still be a loss of personal data depending on when the off-site backup was taken, but having the ability to restore the systems means that while there will be some disruption to the service, the organisation is nevertheless able to comply with this requirement of the DPA.

Are you required to ensure your security measures are effective?

The DPA does not explicitly require you to have a process for regularly testing, assessing, and evaluating the effectiveness of any security measures you put in place. However, having such a process constitutes best practice and will be considered when you are under investigation by the Ombudsman.

What these tests look like, and how regularly you do them, will depend on your own circumstances. However, whatever scope you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as for cybersecurity vulnerability scanning and penetration testing. These are essentially 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve. There are equivalent tests for physical and operational security.

In some industries, you may be required to undertake tests of security measures on a regular basis. While the DPA does not make this an obligation, testing your security measures is considered best practice, depending on the nature of your organisation and the personal data you are processing.

You can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate

safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

What about codes of practice?

If your security measures include a product or service that adheres to a code of practice (once any have been approved), you may be able to use this as an element to demonstrate your compliance with the security – integrity and security principle. It is important that you check carefully that the code is appropriately issued in accordance with section 42 of the DPA.

Apart from any codes of practice, the Ombudsman may, with your consent, assess your processing of personal data for adherence to good practice.

What about your staff?

It is vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, addressing specific security risks which are relevant to your organisation and taking into account the nature and scope of processing your organisation undertakes. Examples of training topics you could consider covering in your training program include:

- your responsibilities as a data controller under the DPA;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognize ‘phishing’ attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

Relevant provisions

Data Protection Act (2021 Revision):¹⁵

Schedule 1, part 1, paragraph 7:	Seventh data protection principle – Security – integrity and security
Schedule 1, part 2, paragraph 3:	Processing contract to ensure reliability
Section 42:	Codes of practice

Further guidance

ICO:	IT security top tips ¹⁶
	IT asset disposal for organisations ¹⁷
	A practical guide to IT security. Ideal for the small business ¹⁸
	Protecting personal data in online services: learning from the mistakes of others ¹⁹
	Bring your own device ²⁰
	Cloud computing ²¹
	Encryption ²²
National Cyber Security Centre:	Technical guidance ²³
UK government:	Cyberaware ²⁴
	Advice for small businesses ²⁵
Data protection guidance of the European Union Agency for Network and Information Security (ENISA) ²⁶	

¹⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

¹⁶ <https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/>

¹⁷ https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

¹⁸ https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

¹⁹ <https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf>

²⁰ https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

²¹ https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

²² <https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/>

²³ <https://www.ncsc.gov.uk/guidance>

²⁴ <https://www.cyberaware.gov.uk/>

²⁵ <https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know>

²⁶ <https://www.enisa.europa.eu/topics/data-protection>

ICO and NCSC:

Guidance on security Outcomes²⁷

Article 29 Working Party:

Guidelines on personal data breach notification²⁸

²⁷ <https://ico.org.uk/for-organisations/security-outcomes/>

²⁸ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Eighth data protection principle - International transfers

At a glance

- The DPA imposes restrictions on the transfer of personal data to countries that are located outside the European Union (EU), and to third countries that do not have adequate protection.
- These restrictions are in place to ensure that the level of protection of individuals afforded by the DPA is not undermined.

In brief

- [Introduction to international transfers](#)
- [What is the international transfers principle?](#)
- [What is an adequate level of protection?](#)
- [Are there any derogations from the prohibition on transfers of personal data outside of the EU or other jurisdictions ensuring adequate protection?](#)
- [What terms will the Ombudsman approve as ensuring adequate safeguards?](#)
- [What authorisations will the Ombudsman make?](#)
- [What steps should I take when I want to use a service provider not based in the Cayman Islands?](#)
- [My service provider's Data Processing Agreement \(DP Agreement\) references EU law. Can I still use it?](#)
- [My service provider won't let me amend the EU Standard Contractual Clauses \(SCCs\) to reference the Cayman DPA. Can I still use them?](#)

Introduction to international transfers

The Cayman Islands has an outside role in the global economy and our businesses are active participants in the global network of international data flows.

Broadly speaking, the eighth data protection principle of the DPA prohibits the international transfer of personal data where the destination does not offer an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This is to ensure that the level of protection guaranteed by the DPA cannot be circumvented by transferring personal data abroad.

This does not mean that personal data cannot be transferred internationally. However, any such transfers need to be assessed against the DPA.

This section seeks to answer common questions data controllers may have about their obligations under the DPA when it comes to transferring personal data and using service providers based outside the Cayman Islands.

What is the international transfers principle?

The eighth data protection principle says:

Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What is an adequate level of protection?

Personal data must not be transferred to another country or territory unless an “adequate level of protection” can be ensured.

For the purposes of the eighth data protection principle, the Ombudsman considers the following countries and territories as ensuring an adequate level of protection:

- Member States of the European Economic Area (that is, the European Union plus Lichtenstein, Norway, and Iceland) where Regulation (EU) 2016/679 (the General Data Protection Regulation or “GDPR”) is applicable;
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) GDPR.

Other countries and territories may still be deemed to have an adequate level of protection depending on:

- the nature of the personal data (eg “Are there sectoral data protection laws that apply?”);
- the country or territory of origin of the information contained in the data;
- the country or territory of final destination of that information;
- the purposes for which and period during which the personal data is intended to be processed;
- the law in force in the country or territory in question;
- the international obligations of that country or territory;
- any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases; and
- any security measures taken in respect of the data in that country or territory.

Note that this listing is not exhaustive. The data controller must conduct a self-assessment of the above elements when deciding whether a country or territory would be compliant with the eighth data protection principle. The data controller will be held accountable for its decision.

Are there any derogations from the prohibition on transfers of personal data outside of the Cayman Islands or other jurisdictions ensuring adequate protection?

The DPA provides derogations from the general prohibition on transfers of personal data outside the Cayman Islands (or other countries officially recognized as offering adequate protections) in certain specific circumstances.

A transfer may be made where it is:

- made with the individual's consent;
- necessary for the performance of a contract between the individual and the organisation, or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of substantial public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject;
- made in regard to public data on a public register, and any conditions subject to which the register is open to inspection are complied with;
- made on terms of a kind approved by the Ombudsman as ensuring adequate safeguards for the individual(s);
- authorised by the Ombudsman as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects; or,
- required under international cooperation arrangements between intelligence agencies or regulatory agencies, if permitted or require under an enactment or an order issued by the Grand Court.

What terms will the Ombudsman approve as ensuring adequate safeguards?

The Ombudsman will approve the following terms as ensuring adequate safeguards:

- data transfer agreements based on standard contractual clauses published by the Ombudsman (forthcoming); or
- data transfer agreements which replicate the rights and obligations contained in the EU 'standard contractual clauses' pursuant to Article 46 paras (2)(c), (2)(d), or (5) GDPR.

Where organisations elect to use standard contractual clauses, the Ombudsman will expect the organisations to amend them accordingly to address the fact that specific cross-references to provisions of European data protection law need to be replaced with cross-references to corresponding provisions of the DPA.

However, we are aware that it may be difficult for some local data controllers to get larger organisations to amend their standard SCCs. We will accept SCCs in the understanding that the intent of the parties is to interpret references to EU law as to the equivalent under the DPA.

The Ombudsman does not consider other types of safeguards specified in Article 46(2) GDPR to automatically qualify as “terms of a kind approved by the Ombudsman” for the purposes of paragraph 8 of Schedule 4 to the DPA. However, transfers of personal data made in accordance with other types of safeguards approved in the European Union in accordance with Article 46 or Article 47 GDPR will be considered favourably by the Ombudsman and will be taken into account in assessing an organisation's compliance with the eighth principle (international transfers).

When will the Ombudsman authorise a transfer?

The Ombudsman may authorise a transfer to which the eighth principle does not apply, if it is nonetheless made in “such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects”.

Where an organisation has been unable to establish, including through a self-assessment using the criteria for adequacy above, that the intended transfer complies with the eighth principle, it can ask the Ombudsman to authorise the transfer in these limited circumstances.

The Ombudsman will expect the data controller to demonstrate appropriate due diligence by, (i) identifying why it is that any departure from the arrangements that are generally considered as adequate in a foreign country is necessary in the particular circumstances of the proposed transfer; and (ii) in respect of each departure identified, explaining and justifying how it is then said that the rights and freedoms of the data subjects can still be adequately protected in these circumstances.

Among other things, the data controller should take into account the following aspects:

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the personal data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases;
- (h) any security measures taken in respect of the data in that country or territory;
- (i) the recipient of the personal data; and
- (j) any relevant rules the recipient is bound by.

The rights and freedoms of the data subject are understood to be the rights identified in the DPA, and could also encompass the rights and freedoms in the Bill of Rights, Freedoms and Responsibilities.

The data controller will be held accountable for its assessment.

What steps should I take when I want to use a service provider not based in the Cayman Islands?

1. Assess whether the country or territory ensures an adequate level of protection:
 - a. Is it a country within the [European Economic Area \(EEA\)](#)? Then the transfer is allowed.
 - b. Is it on the [EU's list of adequate countries](#)? Then the transfer is allowed.
 - c. If not, conduct your own adequacy assessment pursuant to Schedule 1, Part 2 (4) DPA.
2. If adequacy has not been established, do any of the transfer conditions in Schedule 4 DPA apply? These are:
 - a. Consent
 - b. Contract between the data subject and the data controller
 - c. Third-party contract in the interest of the data subject
 - d. Public interest
 - e. Legal proceedings, etc.
 - f. Vital interests
 - g. Public register
 - h. Transfer made on terms approved by the Ombudsman
 - i. Ombudsman has authorised the transfer as being made in "such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects".
 - j. International cooperation between intelligence agencies or regulatory agenciesIf none of the above apply and the transfer is not to an adequate country or territory, a transfer is not permitted. If one of the above applies, a transfer is permitted in principle, subject to the requirements of the next section.
3. Whether through adequacy or a Schedule 4 condition, is the transfer to a data processor or to a data controller?
 - a. If to a data processor, you need to put in place a Data Processing Agreement (DP Agreement).
 - b. If to another data controller, is there a legal basis for the transfer from you to the other data controller? If yes, the transfer is prima facie compliant.

My service provider's Data Processing Agreement (DP Agreement) references EU law. Can I use it?

Yes. We are aware that it may be difficult for some local data controllers to get larger data processors to amend their standard DP Agreements. The requirements for a DP Agreement are quite simple under the DPA, and require merely:

1. A written contract that requires the data processor:
 - a. to act only on instructions from the data controller and
 - b. to ensure appropriate technical and organisational measures to protect the personal data.

These requirements are also found in EU law, so that an EU compliant DP Agreement will also be compliant under Cayman's DPA.

My service provider won't let me amend the EU Standard Contractual Clauses (SCCs) to reference the Cayman DPA. Can I use them?

Yes. We are aware that it may be difficult for some local data controllers to get larger data processors to amend their standard SCCs. We will accept the EU's SCCs on the understanding that the intent of the parties is to interpret references to EU law as to the equivalent under the DPA.

Relevant provisions

Data Protection Act (2021 Revision):²⁹

Schedule 1, part 1, paragraph 8:	Eighth data protection principle – International transfers
Schedule 1, part 2, paragraph 3:	Content of Data Protection Agreement
Schedule 1, part 2, paragraphs 4-6:	Adequate protection, EU findings
Schedule 4:	Transfers to which eighth principle does not apply

Data Protection Regulations, 2018:³⁰

Regulation 10:	Exception to the eighth data protection principle – international cooperation between intelligence and regulatory agencies
----------------	--

²⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

³⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

Further guidance

ICO:	Guidance on international transfers ³¹
European Commission:	Standard contractual clauses – controller to controller (2001) ³² Standard contractual clauses – controller to controller (2004) ³³ Standard contractual clauses – controller to processor (2010) ³⁴
European Data Protection Board:	Guidelines on derogations of Article 49 under Regulation 2016/679 ³⁵

³¹ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/>

³² <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en>

³³ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF>

³⁴ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF>

³⁵ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

Legal basis for processing

In brief

- [What is your legal basis for processing?](#)
- [When is processing “necessary”?](#)
- [How do you decide which legal condition applies?](#)
- [When should you decide your legal basis for processing?](#)
- [What happens if you have a new purpose for processing personal data?](#)
- [How should you document the legal basis of your processing?](#)

What is your legal basis for processing?

The legal bases for processing personal data are set out in schedule 2 of the DPA. Principally, all of the conditions are equal so that none is preferable to any other. At least one of these conditions must apply whenever you process personal data:

- 1) [Consent](#): the individual has given clear consent for you to process their personal data for a specific purpose;
- 2) [Contract](#): the processing is necessary for performance of a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
- 3) [Legal obligation](#): the processing is necessary for you to comply with an Act (not including contractual obligations);
- 4) [Vital interests](#): the processing is necessary to protect the individual’s life;
- 5) [Public functions](#): the processing is necessary for you to perform a public function, or a function of a public nature exercised in the public interest;
- 6) [Legitimate interests](#): Processing necessary for legitimate interests pursued by the data controller or a third party, except where it is unwarranted because of prejudicing the rights and freedoms or legitimate interests of the individual.

The legal bases for processing [sensitive personal data](#) are set out in schedule 3 of the DPA. At least one of these conditions, in addition to a condition for processing above, must apply whenever you process sensitive personal data:

- 1) [Consent](#): the individual has given clear consent for you to process their sensitive personal data for a specific purpose;
- 2) [Employment](#): the processing of sensitive personal data imposed by law in the context of the individual’s employment;

- 3) Vital interests: the processing of sensitive personal data is necessary to protect the vital interests of the individual or any other person where consent cannot be given, cannot reasonably be obtained, or has unreasonably been withheld;
- 4) Non-profit organisations: the processing of sensitive personal data is carried out by certain types of non-profit organisation and relates to individuals who are their members or individuals who are in regular contact with the organisation. This does not cover disclosure to a third party without consent from the individuals concerned;
- 5) Made public: processing of sensitive personal data that has been made public by the individual;
- 6) Legal proceedings: processing of sensitive personal data is necessary for legal proceedings, legal advice or legal rights;
- 7) Public functions: processing of sensitive personal data is necessary for public functions;
- 8) Medical: processing of sensitive personal data by a health professional or someone who owes an equivalent duty of confidentiality is necessary for medical purposes.

When is processing “necessary”?

Many of the legal bases for processing depend on the processing being “necessary”. This means that the processing must be a targeted and proportionate way of achieving the purpose. The legal basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

Example

An application for a credit card requires you to provide the name and contact information of your closest living relative. This information is not necessary for the decision whether to grant or to reject your application.

How do you decide which legal condition applies?

Which legal condition applies will depend on the circumstances and the context of the processing, including these factors:

- What is your purpose of processing – what are you trying to achieve by processing the personal data?

- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?
- Are you a public authority?
- What type of organisation are you?

There is not one-size-fits-all, and there may be more than one applicable legal condition for processing. No one legal condition for processing is better, safer or more important than another, and there is no hierarchy in the listing of the conditions, except to an extent regarding processing necessary for the [exercise of public functions](#).

Several of the legal bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone’s vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in Cayman Islands law, then you are able to use the “public function” basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no prohibition on public authorities using consent or legitimate interests as their lawful basis.

For the purposes of the DPA, the term “public authority” has the same meaning as the definition in the *Freedom of Information Act (2021 Revision)*.

Example

A University that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

The University may be a public authority, so the “public functions” legal basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers.

If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances, considering the factors set out below. For example, a University might rely on “public functions” for processing personal data for teaching and research purposes; but a mixture of “legitimate interests” and “consent” for alumni relations and fundraising purposes.

The University however needs to consider its legal basis for processing carefully – it is the controller’s responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

If you are processing for purposes other than legal obligation, contract, vital interests or public functions, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are the individuals vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?
- To what extent is the processing unavoidable or mandatory?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent. You should avoid relying on consent when the individuals are unable to give a proper consent (see below on conditions for [consent](#)), or the individuals have no genuine choice in the matter.

When should you decide your legal basis for processing?

You should determine your legal basis before starting to process personal data. It's important to get this right the first time. If you find at a later date that your chosen basis was actually inappropriate, it will be more difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis carries a higher risk of being unfair to the individual and lead to breaches of your transparency requirements.

Example

A company decided to process on the basis of consent and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realized that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent.

It is therefore important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should be aware of it.

If there is a genuine change in circumstances or you have a new and unanticipated purpose which means there is a good reason to review your lawful basis and make a change, you need to inform the individual (to the extent it is practicable to do so) and document the change.

What happens if you have a new purpose for processing personal data?

If your purposes change over time or you have a new purpose which you did not originally anticipate, you may not need a new lawful basis as long as your new purpose is compatible with the original purpose.

However, if you rely on consent, you must make sure that the consent is freely given, specific, informed, and unambiguous. Thus, if you want to repurpose personal data which you previously obtained by relying

on consent, you need to either get fresh consent which specifically covers the new purpose or find a different basis for the new purpose. If you do get specific consent for the new purpose, you do not need to show it is compatible with the original purpose.

In other cases, in order to assess whether the new purpose is compatible with the original purpose you should take into account:

- any link between your initial purpose and the new purpose;
- the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – e.g. is it sensitive personal data?;
- the possible consequences of the new processing for individuals; and
- whether there are appropriate safeguards – e.g. encryption or pseudonymization.

This list is not exhaustive and what you need to look at depends on the particular circumstances.

As a general rule, if the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data. You need to identify a new legal basis to process the data for that new purpose.

The DPA specifically says that further processing for the following purposes is considered compatible lawful processing:

- Research purposes ('research' is understood to be scientific research);
- history (archiving) purposes;
- statistical purposes.

There is a link here to the '[purpose limitation](#)' principle in the second data protection principle which states that "Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

How should you document the legal basis of your processing?

Under the DPA you are not required to document upfront that you are in compliance with the Act, or have appropriate policies and processes. However, clear, upfront documentation of all aspects of your personal data processing activities will be very helpful when one of the individuals whose data you process exercises their rights under the Act, when a data breach occurs, or when you are subject of an investigation by the Ombudsman.

Therefore, it is best practice to document the legal basis of all your personal data processing, for each purpose, upfront. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. A good practice would be to include the legal basis in the privacy notice you make available to the data subjects. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

Relevant provisions

Data Protection Act (2021 Revision):³⁶

Schedule 2:	Legal conditions for processing personal data
Schedule 3:	Legal conditions for processing sensitive personal data

Further guidance

ICO:	Lawful basis interactive guidance tool ³⁷
------	--

³⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

³⁷ <https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool/>

Consent

At a glance

- The DPA sets a high standard for consent. However, consent will not always be the appropriate legal basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- If you rely on consent, check your business processes that involve collecting consent and your existing consents. Refresh your consents if they don't meet the DPA standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate and distinguishable from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third-party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Consent to processing cannot be a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.
- Where there is a significant imbalance between the position of the data subject and the data controllers (e.g. in relationship between citizens and public authorities, or relationship between employees and employers) consent may be difficult to qualify as a valid legal basis for processing.

Checklist

Asking for consent

- ☐ We have checked that consent is the most appropriate legal basis for processing.
- ☐ We have made the request for consent prominent and separate from our terms and conditions.
- ☐ We ask people to positively opt in.
- ☐ We don't use pre-ticked boxes or any other type of default consent.
- ☐ We use clear, plain language that is easy to understand.
- ☐ We specify why we want the data and what we're going to do with it.
- ☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- ☐ We name our organisation and any third party controllers who will be relying on the consent.
- ☐ We tell individuals they can withdraw their consent.
- ☐ We ensure that individuals can refuse to consent without detriment.
- ☐ We avoid making consent a precondition of a service.
- ☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- ☐ We keep a record of when and how we got consent from the individual.
- ☐ We keep a record of exactly what they were told at the time.

Managing consent

- ☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- ☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- ☐ We make it easy for individuals to withdraw their consent at any time, and publicize how to do so.
- ☐ We act on withdrawals of consent as soon as we can.
- ☐ We don't penalize individuals who wish to withdraw consent.

In brief

- [Why is consent important?](#)
- [When is consent appropriate?](#)
- [What is valid consent?](#)
- [How should you obtain, record and manage consent?](#)

Why is consent important?

Consent is one of a number of conditions for processing, and explicit consent can also legitimize use of sensitive personal data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimize automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to enforcement actions.

When is consent appropriate?

Consent is one legal basis for processing, but it is not the only legal basis and there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you still plan to process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be a valid legal basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent. This is because consent is unlikely to provide a valid legal basis for the processing where there is a significant imbalance between the data subject and the data controllers.

What is valid consent?

Consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. This means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should you obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. It is best practice to include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Relevant provisions

Data Protection Act (2021 Revision):³⁸

Schedule 2, paragraph 1:	Legal conditions for processing personal data
Schedule 3, paragraph 1:	Legal conditions for processing sensitive personal data
Section 1:	Definition of "consent"
Schedule 5:	Conditions of consent

³⁸ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Further guidance

ICO

Guidance on consent³⁹

Article 29 Working Party

Guidelines on consent under Regulation 2016/679⁴⁰

³⁹ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/>

⁴⁰ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Contract

At a glance

- You can rely on this legal basis if you need to process someone's personal data:
 - to fulfil your contractual obligations to them; or
 - because they have asked you to do something before entering into a contract (e.g. provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this legal basis and ensure that you can justify your reasoning.

In brief

- [What does the DPA say?](#)
- [When can I rely on a contract for processing?](#)
- [When is the legal condition for contracts likely to apply?](#)
- [When is processing 'necessary' for a contract?](#)
- [What else should you consider?](#)

What does the DPA say?

Schedule 2 of the DLP includes a condition for processing of personal data relating to contracts. Paragraph 2 of Schedule 2 says that processing is allowed where:

Processing necessary for contract

2. The processing is necessary for -

- (a) the performance of a contract to which the data subject is a party; or
- (b) the taking of steps at the request of the data subject with a view to entering into a contract.

When can I rely on a contract as a condition for processing?

To rely on this condition for processing, the data subject must be a party to the contract.

If the processing is necessary for the performance of the contract, or in preparation to entering into a contract, you can rely on it.

When is the legal condition for contracts likely to apply?

You meet this legal condition for processing if:

- you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract; or
- you haven't yet got a contract with the individual, but they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask.

It does not apply if you need to process an individual's details who is not party to the contract.

It does not apply if you take pre-contractual steps on your own initiative or at the request of a third party.

Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the age and driving history of the individual.

Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt you should seek your own legal advice.

When is processing 'necessary' for a contract?

The processing must be a targeted and proportionate way of achieving the purpose. This legal basis does not apply if there are other reasonable and less intrusive ways to meet your contractual obligations or take the steps requested.

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this legal basis will not apply and you should consider another legal basis, such as legitimate interests.

Example

When a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

However, the profiling of an individual's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on this condition as the legal basis for this processing. Even if this type of targeted advertising is a useful part of your customer relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you may need to look for a different legal basis as a condition for processing.

What else should you consider?

If the processing is necessary for a contract with the individual, processing is legal on this basis and you do not need to look for a different legal basis.

If processing of sensitive personal data is necessary for the contract, you also need to identify a separate condition for processing this data in Schedule 3. See [below](#) for more on sensitive personal data.

If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected.

If the processing is not necessary for the contract, you need to consider another legal basis such as legitimate interests or consent. Note that if you want to rely on consent you will not generally be able to make the processing a condition of the contract. See more about consent [here](#).

If you are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. See [here](#) for more on automated decision making.

It is best practice to document your decision that processing is necessary for the contract, and include information about your purposes and the legal basis in your [privacy notice](#)

Relevant provisions

Data Protection Act (2021 Revision):⁴¹

Schedule 2, paragraph 2:

Legal conditions for processing

⁴¹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Legal Obligation

At a glance

- You can rely on this condition if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this condition does not apply.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your legal obligation to process the personal data.

In brief

- [What does the DPA say?](#)
- [When is the condition for legal obligation likely to apply?](#)
- [When is processing 'necessary' for compliance?](#)
- [What else should you consider?](#)

What does the DPA say?

Paragraph 3 of Schedule 2 of the DLP provides a legal basis for processing where:

Processing under legal obligation

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

When is the condition for legal obligation likely to apply?

This condition can be relied upon when you are legally obliged to process the personal data to comply with an Act.

The DPA does not specify this, but it is assumed that the Act being relied upon must be applicable in the Cayman Islands. However, this does not have to be an explicit statutory obligation, as long as the application of the Act is foreseeable to those individuals subject to it. As such, it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to the Economics & Statistics Office of the Cayman Islands (“ESO”).

The employer can point to the ESO website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

Example

A financial institution relies on the legal obligation imposed by Part IV of the Anti-Money Laundering Regulations to process personal data in order to undertake customer due diligence, and report suspicious activity to prevent money laundering.

Example

A court order may require you to process personal data for a particular purpose; this also qualifies as a legal obligation.

Mandatory regulatory requirements also qualify as a legal obligation, provided there is a statutory basis underpinning the regulatory regime.

A contractual obligation does not comprise a legal obligation in this context. You cannot contract out of the requirement for a legal basis for processing. However, you can look for a different legal basis. If the contract is with the individual you can consider the legal basis for contracts. For contracts with other parties, you may want to consider legitimate interests.

When is processing 'necessary' for compliance?

The processing must be a targeted and proportionate way of achieving compliance. You cannot rely on this legal basis for processing if you have discretion over whether to process the personal data, or if there is another reasonable way to comply.

It is likely to be clear from the Act in question whether the processing is actually necessary for compliance.

What else should you consider?

If your processing is based on a legal obligation, the [right to stop processing](#) (section 10 of the DPA) does not apply. Read our guidance on individual rights for more information.

Remember to:

- document your decision that processing is necessary for compliance with a legal obligation;
- identify an appropriate source for the obligation in question; and
- include information about your purpose(s) in your [privacy notice](#). Information on the legal basis of processing is not required but it is best practice to include it.

Relevant provisions

Data Protection Act (2021 Revision):⁴²

Schedule 2, paragraph 3: Legal conditions for processing

⁴² https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Vital interests

At a glance

- You are likely to be able to rely on vital interests as your legal basis for processing if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other [sensitive personal data](#) if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

In brief

- [What does the DPA say?](#)
- [What are 'vital interests'?](#)
- [When is the vital interests condition likely to apply?](#)
- [What else should you consider?](#)

What does the DPA say?

Paragraph 4 of Schedule 2 of the DPA says:

Processing to protect vital interests

4. The processing is necessary in order to protect the vital interests of the data subject.

This means that processing personal data is regarded lawful where it is necessary to protect an interest which is essential for the life of the data subject.

What are 'vital interests'?

Vital interests are intended to cover only interests that are essential for someone's life. As such, this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

When is the vital interests condition likely to apply?

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as processing for the exercise of public functions or for legitimate interests is likely to be more appropriate (insofar as Schedule 2 of the DPA is concerned).

Vital interests is also less likely to be the appropriate basis for processing on a larger scale. It might apply where the processing is undertaken on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

However, if you are processing one person's personal data to protect someone else's life, you should generally use an alternative legal basis. For example, in many cases you could consider legitimate interests, which will give you a framework to balance the rights and interests of the data subject(s) with the vital interests of the person or people you are trying to protect.

What else should you consider?

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of sensitive personal data, which means you will also need to identify a condition for processing in Schedule 3 of the DPA. For more on sensitive personal data, see [here](#).

Relevant provisions

Data Protection Act (2021 Revision):⁴³

Schedule 2, paragraph 4:

Legal conditions for processing

⁴³ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

The exercise of public functions

At a glance

- You can rely on this legal basis if you need to process personal data:
 - ‘in the exercise of official authority’. This covers public functions and powers that are set out in law; or
 - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

In brief

- [What does the DPA say?](#)
- [What is the “public functions” condition for processing?](#)
- [What does “public function” mean?](#)
- [Who can rely on the public function basis?](#)
- [What else should you consider?](#)

What does the DPA say?

Paragraph 5 of the DPA says:

Processing necessary for exercise of public functions

5. The processing is necessary for –

(a) the administration of justice;

- (b) the exercise of any functions conferred on any person by or under any enactment;
- (c) the exercise of any functions of the Crown or any public authority; or
- (d) the exercise of any other functions of a public nature exercised in the public interest by any person.

What is the “public functions” condition for processing?

This condition applies to processing necessary for:

- the administration of justice;
- any functions conferred on any person by law;
- the exercise of any functions of the Crown or any public authority;

but also:

- any functions of a public nature exercised in the public interest, even by a person who is not a public authority.

This is not intended as an exhaustive list. If you have other official non-statutory functions or public interest tasks you can still rely on the public function basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other reasonable and less intrusive means to achieve your purpose.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is “necessary” for that purpose.

“Necessary” means that the processing must be a targeted and proportionate way of achieving your purpose. This basis for processing does not apply if there is another reasonable and less intrusive way to achieve the same result.

Your focus should be on demonstrating either that you are carrying out a “public function” in the public interest, or that you are exercising official authority.

What does “public function” mean?

The following factors can help determine whether a function is a public function:

- (a) the extent to which the state has assumed responsibility for the function in question;
- (b) the role and responsibility of the state in relation to the subject matter in question;
- (c) the nature and extent of the public interest in the function in question;
- (d) the nature and extent of any statutory power or duty in relation to the function in question;
- (e) the extent to which the state, directly or indirectly, regulates, supervises or inspects the performance of the function in question;
- (f) the extent to which the state makes payment for the function in question;
- (g) whether the function involves or may involve the use of statutory coercive powers;
- (h) the extent of the risk that improper performance of the function might violate an individual's human rights as set out in the Cayman Islands' Bill of Rights in the Cayman Islands' Constitution.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority.

Who can rely on the public function basis?

Any data controller who is exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

However, if you are a private sector organisation, you may consider the [legitimate interests basis](#) for processing as an alternative.

See the main [legal basis page](#) of this guide for more on how to choose the most appropriate basis.

What else should you consider?

You should consider an alternative legal condition for processing if you are not confident that processing is necessary for a relevant task, function or power.

If you are a public authority (as defined in the DPA), your ability to rely on consent or legitimate interests as an alternative basis is more limited, but they may be available in some circumstances. In particular,

legitimate interests is still available for processing which falls outside your tasks as a public authority. Other legal bases may also be relevant.

Remember that the DPA requires that further processing for other purposes should be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing for:

- archiving purposes in the public interest;
- scientific research purposes; or
- statistical purposes.

If you are processing sensitive personal data, you also need to identify an additional condition for processing this type of data in Schedule 3 of the DPA. Read the [sensitive personal data](#) page of this guide for our latest guidance on these provisions. See [here](#) for more on sensitive personal data.

To help you meet your accountability and transparency obligations, remember to:

- document your decision that the processing is necessary for you to perform a task in the public interest or exercise your official authority;
- identify the relevant task or authority and its basis in common law or statute (where applicable); and
- include basic information about your purposes in your privacy notice. It is best practice also to include the applicable legal conditions for processing.

Relevant provisions

Data Protection Act (2021 Revision): ⁴⁴

Schedule 2, paragraph 5:

Legal conditions for processing

⁴⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Legitimate interests

At a glance

- Legitimate interests is the most flexible legal basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be the most appropriate condition for processing where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests condition. It helps to think of this as a three-part test. You need to:
 - identify a legitimate interest;
 - show that the processing is necessary to achieve it; and
 - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, the legitimate interests condition will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm or prejudice their rights, freedoms, and legitimate interests, the balancing exercise will likely be in favour against the processing.
- Keep a record of your rationale for using this condition to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy notice.

Checklist

- ☐ We have checked that legitimate interests is the most appropriate legal condition.
- ☐ We understand our responsibility to protect the individual's interests.
- ☐ We have conducted an assessment and kept a record of it, to ensure that we can justify our decision.
- ☐ We have identified the relevant legitimate interests served by the processing.
- ☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

- ☐ We have done a balancing test, and are confident that the individual's interests do not override the legitimate interests served by the processing.
- ☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- ☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- ☐ If we process children's data, we take extra care to make sure we protect their interests.
- ☐ We have considered safeguards to reduce the impact of processing under this legal condition where possible.
- ☐ We have considered whether we can offer an opt out.
- ☐ We keep our assessment of relying on this basis under review, and will repeat it if circumstances change.
- ☐ As best practice, we include information about our legitimate interests in our [privacy notice](#).

In brief

- [What is the 'legitimate interests' condition?](#)
- [When can you rely on legitimate interests?](#)
- [How can you apply legitimate interests in practice?](#)
- [What else do you need to consider?](#)

What is the 'legitimate interests' basis for processing?

Paragraph 6 of Schedule 2 of the DPA provides the following condition for processing:

Processing for legitimate interests

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

Examples of activities involving processing which can potentially be justified on the basis of legitimate interest include workplace surveillance, marketing, fraud prevention, intra-group transfers, IT systems monitoring as part of security measures, but this is not an exhaustive list. You may also have a legitimate interest in disclosing information about possible criminal acts or security threats.

‘Necessary’ means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

This basis for processing involves balancing your interests against the individual’s interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual’s interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can you rely on legitimate interests?

Legitimate interests is the most flexible legal basis for personal data processing, but it will not always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people’s rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate condition for processing where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on the legitimate interests condition for marketing activities if you can show that how you use people’s data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object (subject to the individual’s absolute right to opt-out of any [direct marketing](#)).

You can consider legitimate interests for processing data relating to children or vulnerable individuals, but you must take extra care to make sure their interests are protected.

You may be able to rely on the legitimate interests condition in order to legally disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine the lawful condition for their own processing.

You should avoid using the legitimate interests as a legal basis for processing if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people

would object if you explained it to them. You should also avoid this condition if your processing could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

If you are a public authority, you cannot rely on the legitimate interests condition for any processing you do to perform your tasks as a public authority since there is the public functions condition available to you. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider the legitimate interests condition where appropriate. This will be particularly relevant for public authorities with commercial interests.

How can you apply legitimate interests in practice?

If you want to rely on the legitimate interests condition for processing, you can use the three-part test to assess whether it applies. You should do this before you start the processing.

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A legitimate interests assessment (LIA) is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will help you demonstrate compliance in case of a complaint or investigation. In some cases an LIA will be quite short, but in others there will be more to consider.

First, you should identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing? If so, how important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, you should apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, you should do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private? Is the data sensitive personal data, does one of the conditions in Schedule 3 also apply?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing data relating to children or vulnerable individuals?
- Can you adopt any safeguards to minimize the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate legal basis for processing. There is no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it is important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome in case a complaint is raised and the Ombudsman investigates.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another legal condition for processing. Legitimate interests will not often be the most appropriate condition for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a further assessment to assess the risk and potential mitigation in more detail.

What else do you need to consider?

Although it is not required under the DPA, it is best practice to tell people in your [privacy notice](#) what legal condition you rely on to process their data.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights.

Relevant provisions

Data Protection Act (2021 Revision):⁴⁵

Schedule 2, para 6:

Legal conditions for processing

⁴⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Sensitive personal data

At a glance

- “Sensitive personal data” is a defined term within the DPA and covers classes of personal data that warrant extra protection.
- In order to legally process sensitive personal data, you must identify both a legal basis (condition) for processing in Schedule 2 as well as a basis for processing sensitive personal data in Schedule 3 of the DPA. These do not have to be linked, but they may be.
- There are eight conditions for processing sensitive personal data in Schedule 3 of the DPA.
- You must determine your condition for processing sensitive personal data before you begin this processing under the DPA, and you should document it.

In brief

- [What is “sensitive personal data”?](#)
- [What’s different about sensitive personal data?](#)
- [What are the conditions for processing special category data?](#)

What is “sensitive personal data”?

Sensitive personal data is a subset of personal data which carries increased risks. Section 3 of the DPA defines “sensitive personal data” as personal data consisting of:

- (a) the racial or ethnic origin of the data subject;
- (b) the political opinions of the data subject;
- (c) the data subject’s religious beliefs or other beliefs of a similar nature;
- (d) whether the data subject is a member of a trade union;
- (e) genetic data of the data subject;
- (f) the data subject’s physical or mental health or condition;
- (g) medical data;
- (h) the data subject’s sex life;
- (i) the data subject’s commission, or alleged commission, of an offence; or
- (j) any proceedings for any offence committed, or alleged, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

What's different about sensitive personal data?

When processing any of the types of sensitive personal data listed above, you must still satisfy one of the conditions for legal processing in Schedule 2, but you must *also* satisfy one of the conditions in Schedule 3 of the DPA.

This is because the processing of sensitive personal data carries more risks, and so needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Your choice of an applicable legal basis for processing sensitive personal data in Schedule 3 does not dictate which condition you must apply, and vice versa. Instead, you can use any of the conditions in that schedule. You should choose whichever sensitive data condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful condition for processing (in Schedule 2) is vital interests, it is highly likely that corresponding condition for vital interests (in Schedule 3) will also be appropriate.

In assessing whether a particular piece of information is sensitive data will depend on a reasonableness test. For example, the unfounded rumor that a head of state is holding someone hostage in their basement will not be held to be sensitive personal data about the alleged commission of an offence.

What are the conditions for processing sensitive personal data?

The conditions for processing sensitive personal data are listed in Schedule 3. One of these conditions must apply for the processing to be legal, in addition to one of the conditions in Schedule 2. These conditions for processing sensitive personal data are:

1. Consent

The data subject has given consent to the processing of the personal data.

2. Employment

The processing is necessary for the purposes of exercising or performing a right, or obligation, conferred or imposed by law on the data controller in connection with the data subject's employment.

3. Vital interests

The processing is necessary -

(a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. Non-profit associations

The processing -

(a) is carried out in the course of its legitimate activities by a body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade union purposes;

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;

(c) relates only to data subjects who are members of the body or association or have regular contact with it in connection with its purposes; and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. Information made public by data subject

The information contained in the personal data has been made public as a result of steps taken by the data subject.

6. Legal proceedings, etc.

The processing -

(a) is necessary for the purpose of, or in connection with, any legal proceedings;

(b) is necessary for the purpose of obtaining legal advice; or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. Public functions

The processing is necessary for -

(a) the administration of justice;

(b) the exercise of any functions conferred on any person by or under an enactment; or

(c) the exercise of any functions of the Crown or any public authority.

8. Medical purposes

(1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional; or

(b) a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.

(2) In this paragraph, “medical purposes” includes the purposes of preventative medicine, medical diagnosis, the provision of care and treatment and the management of healthcare services.

Relevant provisions

Data Protection Act (2021 Revision): ⁴⁶

Section 3: Definition of “sensitive personal data”

Schedule 3: Conditions for processing sensitive personal data

Further guidance

Relevant provisions in the GDPR:⁴⁷ Article 9(2) and Recital 51

⁴⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁴⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Individual rights

Under the DPA individuals have rights in relation to their own personal data. These rights are not absolute as they may be restricted in certain specified circumstances. Exemptions may also apply, whereby specified rights or other provisions of the DPA do not apply.

The DPA grants the following rights to individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to stop/restrict processing
- The right to stop direct marketing
- The rights in relation to automated decision making
- The right to seek compensation
- The right to complain

The right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the DPA.
- You must provide individuals with information including:
 - who the data controller is; and
 - your purpose(s) for processing their personal data.

This is called “privacy information” and is usually communicated in a “privacy notice”.

- You must provide privacy information to individuals “as soon as reasonably practicable”, which generally means at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data, either directly or indirectly through

a public notice, depending on the processing activity and the ability to directly notify the individuals.

- There are circumstances when you are not obliged to provide the privacy information.
- You should regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to the attention of the individuals before you start processing their data.
- Getting the right to be informed correct can help you to comply with other aspects of the DPA and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklist

What to provide

We provide individuals with all the following privacy information:

- ☐ The name and contact details of our organisation; and
- ☐ The purposes of the processing.

When to provide it

- ☐ We provide individuals with privacy information at the time we collect their personal data from them (or as soon as possible afterward if it is not reasonably practicable to give notice upfront).
- ☐ If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information within a reasonable of period (or make it easily accessible, e.g. on our website, if it is not reasonably practicable to directly contact the individual).

How to provide it

We provide the information in a way that is:

- ☐ concise;
- ☐ transparent;
- ☐ intelligible;
- ☐ easily accessible; and
- ☐ uses clear and plain language.

Changes to the information

- ☐ We regularly review and, where necessary, update our privacy information.

- ☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

- ☐ We undertake an information audit to find out what personal data we hold and what we do with it. The results may be recorded in a record of processing activities (RoPA).
- ☐ We put ourselves in the position of the people we’re collecting information about.
- ☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- ☐ a layered approach;
- ☐ dashboards;
- ☐ just-in-time notices;
- ☐ icons; and
- ☐ mobile and smart device functionalities.

In Brief

- [What is the right to be informed and why is it important?](#)
- [What privacy information should you provide to individuals?](#)
- [When should you provide privacy information to individuals?](#)
- [What are the exemptions to the right to be informed?](#)
- [Should you test, review and update our privacy information?](#)
- [The right to be informed in practice](#)

What is the right to be informed and why is it important?

The right to be informed covers a key transparency requirement of the DPA. It is about providing individuals with a privacy notice that contains clear and concise information about who you are and what you do with their personal data.

Using an effective approach can help you to comply with other aspects of the DPA, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to complaints, investigation and fines, and may lead to reputational damage.

What privacy information should you provide to individuals?

You are required to provide:

- your own identity; and
- the purpose(s) of processing.

It is best practice (but optional under the DPA) to provide additional information, such as:

- your organisation's contact details;
- your representative's contact details (if applicable);
- the legal basis of processing (including statutory requirements if applicable);
- the legitimate interests of processing (if applicable);
- the categories of data obtained;
- the source of the data;
- the recipients or categories of recipients of the data;
- the details of any international transfers;
- the retention period of the data;
- the rights available to individuals;
- the right and contact details to make a complaint to the Ombudsman; and
- the details of any automated decision making.

What you should tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

Additionally, a lot of best practice information will be required information under a [Subject Access Request](#) (SAR). Consequently, you may be able to reduce the number of SARs you receive and need to respond to by having an expanded, best practice privacy notice.

When should you provide privacy information to individuals?

When you collect personal data from the individuals it relates to, you must provide them with privacy information as soon as reasonably practicable. In most cases this will mean before or at the time you obtain their data, but where it is not practicable to do so, you should provide the privacy information as soon as possible after you have collected their personal data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information as soon as reasonably practicable. This is not further specified in the Act, but is taken to mean within a reasonable period of time, such as within a month, whenever you first communicate with the individual, or whenever you first disclose the data to someone else.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

Where direct interaction with the individuals concerned is not possible or reasonably practicable, you should still take steps to make sure that your privacy information is at least readily and publicly accessible (e.g. through a privacy notice posted on your website).

What are the exemptions to the right to be informed?

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

The DPA recognizes the following exemptions from the right to be informed:⁴⁸

- Section 19: the data is processed for crime prevention, detection or investigation, the apprehension or prosecution of any person suspected of having committed an offence, or the assessment or collection of any fees or duty;
- Section 21: the data is processed for monitoring, inspection or a regulatory function, to the extent that applying it would be likely to prejudice the discharge of the function;
- Section 23: the data is processed for statistical purposes or for the purposes of historical or scientific research;
- Section 24: the data consists of information you are obliged by law to make available to the public;
- Section 27: the data is processed for purposes of conferring any honour or dignity by the Crown or the Premier;
- Section 28: the data is processed for purposes of corporate finance and the application of the provision could affect the price of a financial instrument, or for the purpose of safeguarding an important economic or financial interest of the Cayman Islands;
- Section 29: the data consists of intentions in regard to any negotiations with the individual which would be prejudiced by the processing;
- Section 30: the processed data consists of information in respect of which legal professional privilege applies and in respect of trusts and wills;
- Regulation 7: the notification could reasonably cause mental or physical harm to any person;

⁴⁸ See more on exemptions [here](#).

- Regulation 9: to the extent that the notification would be likely to prejudice the carrying out of social work because of serious harm to the physical or mental health or condition of any person.

For more details on these and other exemptions, see [here](#).

How should you draft your privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

How should you provide privacy information to individuals?

There are a number of techniques you can use to provide people with privacy information. You can use:

- **A layered approach** – typically, short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.

- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.

Should you test, review and update your privacy information?

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalized, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

The right to be informed in practice

If you **sell** personal data to (or **share** it with) other organisations:

- As part of the privacy information you provide, you must tell people that you plan to sell or share the information, and also who you are giving their information to, unless you are relying on an exception or an exemption.
- You can tell people the names of the organisations or the categories that they fall within; choose the option that is most meaningful.
- It is good practice to use a dashboard to let people manage who their data is sold to, or shared with, where they have a choice.

If you **buy** personal data from other organisations:

- You must provide people with your own privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, it is best practice to carry out a privacy impact assessment to find ways to mitigate the risks of the processing.

- If your purpose for using the personal data is different to that for which it was originally obtained, you must tell people about this. It is best practice to also tell them what your legal basis is for the processing.
- Provide people as soon as practicable with your privacy information after buying the data.

If you obtain personal data from **publicly accessible sources**:

- You still have to provide people with privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, it is best practice to carry out a privacy impact assessment to find ways to mitigate the risks of the processing.
- Be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from a number of different sources. Remember that you still need a legal basis for the intended processing.
- Provide people with privacy information as soon as practicable after obtaining the data.

If you apply **Artificial Intelligence (AI)** to personal data:

- Be upfront about it and explain your purposes for using AI.
- If the purposes for processing are unclear at the outset, give people an indication of what you are going to do with their data. As your processing purposes become clearer, update your privacy information and actively communicate this to people.
- Inform people about any new uses of personal data before you actually start the processing.
- If you use AI to make solely [automated decisions](#) about people with legal or similarly significant effects, tell them what information you use, why it is relevant and what the likely impact is going to be.
- Consider using just-in-time notices and dashboards which can help to keep people informed and let them control further uses of their personal data.

Relevant provisions

Data Protection Act (2021 Revision):⁴⁹

Schedule 1, part 2, paragraph 2:	Specified information at relevant time
Section 19(2):	Exemption relating to crime, government fees and duties
Section 23(2):	Exemption relating to research, history or statistics

⁴⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Data Protection Regulations, 2018:⁵⁰

Regulation 7(1): Exemption relating to health

Regulation 9(1): Exemption relating to social work

Further guidance

Article 29 Working Party Guidelines on Transparency under Regulation 2016/679⁵¹

ICO Guidance on the right to be informed⁵²

Guidance on Data Protection Impact Assessments.⁵³

⁵⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

⁵¹ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

⁵² <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/>

⁵³ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

The right of access

At a glance

- Individuals have the right to access their own personal data.
- This is commonly referred to as subject access.
- To do so, individuals must make a subject access request (“SAR”) in writing.
- You have thirty days to respond to a request.
- If you need further information from the requestor, the period of time for your response can be extended by the Regulations.
- There is no fee to deal with a request except in exceptional circumstances.

Checklist

Preparing for subject access requests:

- ☐ We know how to recognize a subject access request and we understand when the right of access applies.
- ☐ We have a policy to record the requests we receive.
- ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- ☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests:

- ☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within thirty days of receipt.
- ☐ We are aware of the circumstances when we can extend the time limit to respond to a request.
- ☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
- ☐ We understand what we need to consider if a request includes information about others.

In brief

- [What is the right of access?](#)
- [What is an individual entitled to?](#)
- [Personal data of the individual and mixed personal data](#)
- [How do you recognize a request?](#)
- [Should you provide a specially designed form for individuals to make a subject access request?](#)
- [How should you provide the data to individuals?](#)
- [What if the data is already open to access?](#)
- [Do you have to explain the contents of the information you provide to the individual?](#)
- [Can you charge a fee?](#)
- [How long do you have to comply with a subject access request?](#)
- [Can you extend the time for a response?](#)
- [Can you ask an individual for ID?](#)
- [What about requests for large amounts of personal data?](#)
- [What about requests made on behalf of others?](#)
- [What about requests for information about children?](#)
- [What should you do if the data includes information about other people?](#)
- [If we use a processor, does this mean they would have to deal with any subject access requests you receive?](#)
- [Can you refuse to comply with a subject access request?](#)
- [What are the exemptions to the right of access?](#)
- [What should you do if you refuse to comply with a request?](#)

What is the right of access?

The right of access, commonly referred to as subject access or as a Subject Access Request (SAR), gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

What is an individual entitled to?

The DPA provides that individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this includes the information you should provide in a privacy notice, but also additional information.

In addition to a copy of their personal data, you also must provide individuals with the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or classes of recipient you disclose, or may disclose, the personal data to;
- any countries or territories outside the Cayman Islands to which you do, or intend to, transfer the personal data;
- the general measures you take to ensure the security of the personal data (i.e. to comply with the seventh data protection principle);
- any information available as to the source of the personal data;
- the reasons for any automated decision made in relation to the individual, including the individual's performance at work, creditworthiness, reliability or conduct; and
- the right to make a complaint to the Ombudsman.

You may have provided some of this information already in your privacy notice.

A subject access request does not need to be for all the types of information listed above. However, you should clarify to the requestor that they are entitled to the types of information listed above.

For instance, a requestor may only be interested in receiving one type of information you hold, instead of all personal data held.

Personal data of the individual and mixed personal data

An individual is only entitled to their own personal data and certain information about the data, but not to information relating to other people (unless the information is also about the individual or the individual is acting on behalf of someone else). Therefore, it is important that you establish whether the information requested falls within the [definition of personal data](#).

Sometimes, you will come across so-called "mixed personal data", i.e. where personal data of one data subject is very closely linked to the personal data of another data subject. If the third party data subject has not consented to the disclosure of the mixed personal data, you will need to assess whether the mixed personal data will need to be redacted or whether it can be released as mixed personal data.

Example

An individual makes a request for their personal data consisting of the recording of a phone call between the data subject and an employee of the data controller. The recording contains personal data relating to both the data subject and the employee.

Unless the employee has consented to the disclosure of the mixed personal data of the recording, the data controller will need to assess whether the overall circumstances call for the data controller to redact the phone call in order to not disclose personal data of the employee or whether the circumstances may permit a disclosure of the mixed personal data to the data subject.

You need to assess whether it is reasonable in all circumstances to disclose the mixed personal data. In particular, this will require the data controller to balance the respective interests of the affected data subjects, including:

- whether a duty of confidentiality towards the other data subject is owed;
- what type of the personal data would be disclosed;
- whether any steps were taken by the data controller to seek consent of the other data subject;
- whether the other data subject is capable of granting consent; and
- whether the other data subject has expressly refused consent.

The issue of mixed personal data is addressed in section 8(7)-(10) DPA.

How do you recognize a request?

The DPA specifies that a subject access request must be made in writing.

A request does not have to include the phrase 'subject access request' or section 8 of the DPA, as long as it is clear that the individual is asking for their own personal data.

This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a subject access request.

Additionally, it is good practice to have a policy for recording details of the requests you receive. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Should you provide a specially designed form for individuals to make a subject access request?

Standard forms can make it easier both for you to recognize a subject access request and for the individual to include all the details you might need to locate the information they want.

However, even if you have a form, you should note that a subject access request is valid if it is submitted in writing by any means, e.g. in hardcopy letter, by email, etc., so you will still need to comply with any requests you receive in any written format.

Therefore, although you may invite individuals to use a form, you must make it clear that it is optional. You should not try to use this as a way of extending the thirty-day time limit for responding.

How should you provide the data to individuals?

The DPA specifies that data should be provided in the format requested by the individual, unless:

- the supply of such a copy is not possible or would involve disproportionate effort, or
- the data subject agrees otherwise.

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

Where possible, it is best practice to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will not be appropriate for all organisations, but there are some sectors where this may work well.

However, providing remote access should not adversely affect the rights and freedoms of others – including trade secrets or intellectual property.

What if the data is already open to access?

If the data is open to access by the public by law or as part of a public register, you should refer the requestor there.

If the data is available for purchase by the public in accordance with administrative procedures established for that purpose, the data must be obtained in accordance with those procedures.

You have received a request but need to amend the data before sending out the response. Should you send out the “old” version?

Strictly speaking, a subject access request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it would be reasonable for you to supply information you hold when you send out a response, even if this is different to that held when you received the request.

However, it is not acceptable to amend or delete the data if you would not otherwise have done so.

Under the DPA it is an offence to fail to supply, alter, suppress or destroy information that is required to be produced to the Ombudsman.

Do you have to explain the contents of the information you provide to the individual?

The DPA requires that the information you provide to an individual is in an intelligible form, which means using clear and plain language. This may be particularly important where the information is addressed to a child, or if you are a business dealing with consumers who may not be familiar with any technical terms used within documents containing personal data.

If the personal data themselves are not understandable without an explanation (e.g. because the data is coded), they must be provided accompanied by an adequate explanation.

At its most basic, this means that the information you provide in response to a request should be capable of being understood by an average person (or child). However, you are not required to ensure that the information is provided in a form that can be understood by the particular individual making the request.

For further information about requests made by a child please see the 'What about requests for information about children?' section [below](#).

Example

An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to your key or index to explain this information, it would be impossible for anyone outside your organisation to understand. In this case, you are required to explain the meaning of the coded information. However, although it is good practice to do so, you are not required to decipher poorly written notes if you only have these notes and no clearer version, as the DPA does not require you to make information legible.

Example

You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. You are not required to do this even if the person who receives it cannot understand all of it because it can be understood by the average person. However, it is good practice for you to help individuals understand the information you hold about them.

Can you charge a fee?

The personal data you have to provide following a request must be provided free of charge.

However, the Regulations provide that where the request is manifestly unfounded or excessive you may charge a reasonable fee for the costs of providing the requested data and information, or refuse to act on the request.

This will only be in very few cases, since the DPA defines a request that is “manifestly unfounded or excessive” as a request that:

- is repetitive;
- is fraudulent in nature; or
- would divert the resources of the data controller unreasonably,

As the data controller you have the burden of proving that a request is “manifestly unfounded” or “excessive”. In the event of disagreement, the Ombudsman shall decide on the facts.

How long do you have to comply with a subject access request?

You must comply with a subject access request within thirty days from the date when you receive the request.

You should calculate the time limit as thirty days from the day after you receive the request (whether the day after is a working day or not).

If you have asked for a fee or further clarification from the individual (e.g. proof of identity), this may suspend the period for responding. The period resumes when the fee and/or further information has been supplied.

The period for responding to the request begins when you receive the additional information. However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 3 October to comply with the request, (i.e. thirty days after the request was received).

Can you extend the time for a response?

Regulation 4 (1) provides that you can extend the time to respond to a request for up to thirty additional days, if:

- a large amount of data is requested or is required to be searched and meeting the timelines would unreasonably interfere with your operations;
- more time is required to consult with a third party or other data controller before you are able to decide whether or not to give the requestor access to the requested data; or
- the data subject has given consent to the extension.

If you extend, the period for responding to a request, you must inform the requestor, and provide reasons for the extension.

It is the Ombudsman's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Regulation 4 (2) provides that, with the permission of the Ombudsman, you can extend the period for responding to a request by more than thirty days, if:

- one or more of the circumstances described above apply; and
- the Ombudsman considers that it is appropriate to do so.

If you believe you need to extend the period for responding to a requestor for more than thirty days, you should contact the Office of the Ombudsman with all the details, and request an extension in writing.

Can you ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.

You need to let the individual know as soon as possible if you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

While you may need to confirm the identity of the person making the request, this does not mean you are always justified to keep a copy the information provided, due to the [third](#) and [fifth](#) data protection principles.

What about requests for large amounts of personal data?

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.

You need to let the individual know as soon as possible that you need more information from them before responding to their request.

Where the request is manifestly unfounded or excessive because the request “would divert the resources of the data controller unreasonably”, you can:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case you need to justify your decision

See [above](#) for more on charging a fee in certain circumstances.

What about requests made on behalf of others?

The DPA does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party’s responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Example

A bank has an elderly customer who visits a particular branch to make weekly withdrawals from one of her accounts. Over the past few years, she has always been accompanied by her daughter who is also a customer of the branch. The daughter makes a subject access request on behalf of her mother and explains that her mother does not feel up to making the request herself as she does not understand the ins and outs of data protection. As the information held by the bank is mostly financial, it is rightly cautious about giving customer information to a third party. If the daughter has been appointed by the court to manage her mother’s affairs, the bank would be happy to comply. They ask the daughter whether she has such a power, but she does not.

Bearing in mind that the branch staff know the daughter and have some knowledge of the relationship she has with her mother, they might consider complying with the request by making a voluntary

disclosure, if permitted under banking law. However, the bank is not obliged to do so, and it would not be unreasonable to require more formal authority.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual may not be able to manage their own affairs because they do not have the mental capacity to do so, or for another reason. Such individuals should be represented by a court-appointed guardian who can request access to their data on behalf of the data subject.

The exemption relating to education in the DP Regulations provides that where the data is an educational record that consists of information that a child has been subject to abuse, or may be at risk of it, the right to access by a parent or someone appointed by the court to manage the individual's affairs does not apply if it would not be in the interests of the child.

The exemption relating to social work in the DP Regulations also restricts the application of the right to access exercised on behalf of a data subject by a parent or someone appointed by the court, if the information was initially provided to the data controller in the expectation that the data would not be disclosed to the person making the request (unless the data subject has indicated they do not have this expectation any longer).

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. It is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;

- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

The Regulations define a child as a person under the age of eighteen years old.

See also the exemption on [social work](#) and [education](#).

What should you do if the data includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

The DPA says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

Data about a third party individual may include information on the source of the personal data. However, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data

subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

This does not mean that you are excused from communicating as much of the personal data sought in the request as can be communicated without disclosing the identity of the other (third party) individual. This can be done by redacting or omitting the names or other identifying particulars from the data.

If we use a processor, does this mean they would have to deal with any subject access requests you receive?

Responsibility for complying with a subject access request lies with you as the controller. You need to ensure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you directly, or to the processor who acts on your behalf. For more on contracts with processors [here](#).

You are not able to extend the one-month time limit on the basis that you have to rely on a processor to provide the information that you need to respond. As mentioned above, the Regulations allow you to extend the time limit only for another thirty days if:

- a large amount of data is requested or required to be searched and meeting the deadline would unreasonably interfere with your other operations;
- more time is required to consult with a third party or other data controller to decide on access; or
- the data subject has agreed with the extension.

In exceptional circumstances, if even more time is needed the timelines can be extended further, but only with the permission of the Ombudsman.

Can you refuse to comply with a subject access request?

The Regulations provide that you can refuse to comply with a subject access request if it is manifestly unfounded or excessive because the request:

- is repetitive;
- is fraudulent in nature, or
- would divert the resources of the data controller unreasonably.

If you consider that a request is manifestly unfounded or excessive you can:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case you need to justify your decision. In the case of disagreement, the Ombudsman shall decide on the facts.

As well, if the data is already available by law as part of a public register or otherwise, or for sale under administrative procedures, you must provide access under those administrative procedures and not under the DPA.

What are the exemptions to the right to access?

The DPA recognizes the following exemptions from the right to access: ⁵⁴

- Section 19: if the personal data is processed for crime prevention, detection or investigation, the apprehension or prosecution of any person suspected of having committed an offence, or the assessment or collection of any fees or duty;
- Section 21: if the personal data is processed for monitoring, inspection or a regulatory function, to the extent that applying it would be likely to prejudice the discharge of the function;
- Section 24: if the data consists of information you are obliged by law to make available to the public;
- Section 27: if the personal data is processed for purposes of conferring any honour or dignity by the Crown or the Premier;
- Section 28: if the data is processed for purposes of corporate finance and the application of the provision could affect the price of a financial instrument, or for the purpose of safeguarding an important economic or financial interest of the Cayman Islands;
- Section 29: if the personal data consists of intentions in regard to any negotiations with the individual which would be prejudiced by the processing;
- Section 30: if the personal data is being processed for legal or trust purposes;
- Regulation 7: if the release of personal data could reasonably cause mental or physical harm to any person; or
- Regulation 9: to the extent that the notification would be likely to prejudice the carrying out of social work because of serious harm to the physical or mental health or condition of any person.

What should you do if you refuse to comply with a request?

You must inform the individual that you refuse to comply with the request without undue delay.

You should inform the individual about:

- the reasons you are not taking action;

⁵⁴ See more on exemptions [below](#).

- their right to make a complaint to the Ombudsman; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

Relevant provisions

Data Protection Act (2021 Revision):⁵⁵

Sections 8-9: Right to access

Data Protection Regulations, 2018:⁵⁶

Regulation 3 Fees for requests

Regulation 4: Extension of time for response

Regulation 6: Additional circumstances when the data controller does not have to comply with a request under section 10 (right to stop processing)

⁵⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁵⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

The right to rectification

At a glance

- The fourth data protection principle (the data accuracy principle) requires that data controllers ensure personal data is accurate and, where necessary, up to date.
- The DPA includes, indirectly, a right for individuals to have inaccurate personal data rectified or completed if it is incomplete, insofar as the data controller is convinced of the validity of the request. Although there is no explicit legal obligation for the data controller to act on a direct request for rectification from an individual, as a matter of fairness derived from the first data protection principle, and also as a consequence of the fourth data protection principle (data accuracy), data controllers should correct inaccurate data and update outdated data without undue delay.
- An individual can complain to the Ombudsman, who may issue an order for rectification, blocking, erasure or destruction of the data in question where the complaint is upheld.
- In certain circumstances a request for rectification can be refused.

Checklist

Preparing for requests for rectification

- ☐ We know how to recognize a request for rectification and we understand when this right applies.
- ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for rectification

- ☐ We have processes in place to ensure that we respond to a request for rectification without undue delay.
- ☐ We have appropriate systems to rectify or complete information, or provide a supplementary statement.
- ☐ We have procedures in place to inform any recipients if we rectify any data we have shared with them.

In brief

- [What is the right to rectification?](#)
- [What do you need to do?](#)
- [When is data inaccurate?](#)
- [What should you do about data that records a mistake?](#)
- [What should you do about data that records a disputed opinion?](#)
- [What should you do while you are considering the accuracy?](#)
- [What should you do if you disagree with the request for rectification?](#)
- [How can you recognize a request?](#)
- [Can you charge a fee?](#)
- [How long do you have to comply?](#)
- [Can you ask an individual for ID?](#)
- [Do you have to tell other organisations if you rectify personal data?](#)

What is the right to rectification?

Under sections 14 and 43 of the DPA individuals have the right to complain to the Ombudsman and have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

However, you may have already taken steps to correct inaccurate data when an individual brought it to your attention.

This right has close links to the fourth data protection principle (the data accuracy principle) in Schedule 1 of the DPA which requires that data controllers keep the personal data they are processing accurate and, where necessary, up to date. See more on the fourth data protection principle [here](#).

In some circumstances the right to rectification may also be linked with the individual's [right to stop or restrict the processing](#).

What do you need to do?

If you receive a request for rectification you should take reasonable steps to satisfy yourself whether the data is accurate and to rectify or update the data, if necessary. You should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a

greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

You are not obligated to correct inaccurate personal data, unless you are ordered to do so by the Ombudsman. However, it makes sense to do so when possible.

When is data inaccurate?

Section 2 of the DPA defines inaccuracy of data as follows:

“inaccurate”, in relation to personal data, includes data that are misleading, incomplete or out of date

What should you do about data that records a mistake?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data. Indeed, in some cases it may be necessary to preserve inaccurate or incomplete personal data, for example as part of record of audit, or record of complaints handling.

Example

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. While the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it may be difficult to argue that the record is inaccurate and should be rectified.

What should you do about data that records a disputed opinion?

Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

Can you keep processing data while you are considering their accuracy?

If an individual tells you that personal data is inaccurate or (where applicable) out of date, you should verify whether that is true. As a matter of best practice, you should restrict the processing of the personal data in question while you are verifying its accuracy, whether or not the individual has exercised their right to restriction.

The same approach should be practiced while the complaint is under investigation by the Ombudsman, until she has reached conclusions in the matter.

What should you do if you disagree with the request for rectification?

While in regard to a request for access under section 8 of the DPA you can refuse to act if the request is manifestly unfounded or excessive,⁵⁷ the DPA does not provide for reasons for refusing a request for rectification.

You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to complain to the Ombudsman, and their ability to seek to enforce their rights through a judicial remedy.

It is best practice to place a note on your system or file indicating that the individual challenges the accuracy of the data and their reasons for doing so.

⁵⁷ See more on the right to access [here](#).

What are the exemptions to the right to rectification?

The DPA recognizes the following exemptions from the right to rectification: ⁵⁸

- Section 18: exemption relating to national security;
- Section 24: exemption relating to information available to the public by law;
- Section 25: exemption relating to disclosure required by law or made in connection with legal proceedings; and
- Section 26: exemption relating to personal, family or household affairs.

How can you recognize a request for rectification?

The DPA does not specify how to make a request for rectification. An individual can make a request for rectification verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or the fourth data protection principle of the DPA to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request.

This presents a challenge as any of your employees could receive a valid verbal request. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is best practice to have a policy for recording details of the requests you receive in a log, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Can you charge a fee for responding to a request for rectification?

No, you cannot charge a fee to comply with a request for rectification.

While in regard to a request for access under section 8 of the DPA you can charge a reasonable fee if the request is manifestly unfounded or excessive because it would divert your resources unreasonably, ⁵⁹ the DPA does not provide for any fee to be charged in connection with a request for rectification.

⁵⁸ See more on exemptions [here](#).

⁵⁹ See more on the right to access [here](#).

How long do you have to comply with a request for rectification?

The DPA does not set any procedures or timelines for your response to a request for rectification. Instead it anticipates that the individual complains to the Ombudsman who may then investigate and issue an order where appropriate.

Can you ask an individual for ID when they make a request for rectification?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You should let the individual know without undue delay that you need more information from them to confirm their identity.

Do you have to tell other organisations if you rectify personal data?

If you have disclosed the inaccurate personal data to third parties, you should contact each third party and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these third parties.

The DPA defines a third party as follows:

“third party”, in relation to personal data, means any person other than -
(a) the data subject;
(b) the data controller; or
(c) any data processor or other person authorised to process data for the data controller or data processor.

If the Ombudsman makes an order for data rectification, she may order you to notify third parties to whom the data has been disclosed of the rectification, if it is considered reasonable practicable.

You will remain responsible for the accuracy of any processing conducted by your processors.

Relevant provisions

Data Protection Act (2021 Revision):⁶⁰

Schedule 1, part 1, paragraph 4:	Fourth data protection principle – Data accuracy
Section 14:	Rectification, blocking, erasure or destruction
Section 43:	Complaints to the Ombudsman
Section 45:	Enforcement orders

Data Protection Regulations, 2018:⁶¹

Regulation 3	Fees for requests
--------------	-------------------

⁶⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁶¹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

The right to stop or restrict processing

At a glance

- Individuals have the right to require that processing stop, or not begin, or cease processing for a specified purpose or in a specified way.
- This is not an absolute right and does not apply in certain circumstances.
- An individual must make a request to stop processing in writing.
- You have one twenty-one days to respond to a request, or apply to the Ombudsman not to comply with the request.
- This right has close links to other rights, including the [right to rectification](#) (the fourth data protection principle) and the [right to object to direct marketing](#) (section 11 of the DPA).

Checklist

Preparing for requests to stop or restrict processing

- ☐ We know how to recognize a request to stop or restrict processing and we understand when the right applies.
- ☐ We have a log in place to record requests.
- ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests to stop or restrict processing

- ☐ We have processes in place to ensure that we respond to a request to stop or restrict processing without undue delay and within twenty-one days of receipt.
- ☐ We have appropriate methods in place to stop or restrict the processing of personal data on our systems.
- ☐ We have appropriate methods in place to indicate on our systems that processing has been restricted.
- ☐ We understand we need to apply to the Ombudsman not to comply with a request to stop or restrict processing.
- ☐ We have procedures in place to inform any recipients if we stop or restrict any data we have shared with them.

In brief

- [What is the right to stop or restrict processing?](#)
- [When does the right to stop or restrict processing apply?](#)
- [How do you stop or restrict processing?](#)
- [Can you do anything with restricted data?](#)
- [Do you have to tell other organisations about ceasing or restricting processing of personal data following a request from an individual?](#)
- [Can you refuse to comply with a request to cease or restrict processing?](#)
- [What are the exemptions to the right to stop or restrict processing?](#)
- [How do you recognize a request to stop or restrict processing?](#)
- [Can you charge a fee for responding to a request to stop or restrict processing?](#)
- [How long do you have to comply with a request to stop or restrict processing?](#)
- [Can you ask an individual for ID?](#)

What is the right to stop or restrict processing?

Section 10 of the DPA gives individuals the right to require organisations that process their personal data to stop processing, not begin processing, or cease processing for a specified purpose or in a specified way.

This means that an individual can stop or limit the way that a data controller uses their data. This includes the erasure of their data.

Individuals have to notify you in writing, but they do not have to state a reason to have the right to stop or restrict the processing of their personal data.

This right does not apply in all circumstances. There are also certain exemptions from the right to stop or restrict processing.

The individual may agree to impose the restriction for a certain period of time.

When does the right to stop or restrict processing apply?

Individuals have the right to demand that you stop processing, not begin processing, or cease processing their personal data for a specified purpose or in a specified way.

However, you do not have to comply with a request to stop or restrict processing if:

- the processing is necessary for performance of a contract to which the individual is a party (or taking steps at the request of the individual towards entering into a contract;
- the processing is necessary under a legal obligation to which the data controller is subject;
- the processing is necessary to protect the vital interests of the individual; or

- you have requested and received the approval of the Ombudsman.

Although this is distinct from the right to rectification and the right to object to direct marketing, there are close links between those rights and the right to stop or restrict processing:

- under section 14 of the DPA individuals have the right to complain to the Ombudsman, and the Ombudsman may order that the personal data be blocked, erased or destroyed (as well as rectified); and
- under section 11 of the DPA individuals have the right to object to direct marketing.

As a matter of best practice you should automatically temporarily restrict the processing while you or the Ombudsman are considering the request or complaint.

How do you stop or restrict processing?

You need to have processes in place that enable you to stop or restrict processing personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

Depending on the circumstances, if the request is to cease processing personal data for a specified purpose, in a specified way, or for a certain period of time, you may have to:

- temporarily move the data to another processing system;
- make the data unavailable to users; or
- temporarily remove published data from a website.

If the individual has asked you not to erase the data, it is particularly important that you consider how you store personal data that you no longer need to process otherwise.

If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed while the restriction is in place. You should also note on your system that the processing of this data has been restricted.

Can you do anything with restricted data?

Depending on the nature of the restriction the individual requested, you may not be able to process the data at all, and it should be erased. This is the case unless:

- the individual has not demanded that you stop processing their data outright, but that you cease processing their personal data for a specified purpose or in a specified way only;

- the data is being processed in the context of a contract, a legal obligation or to protect the vital interests of the individual; or
- an exemption applies to the processing you undertake.⁶²

You can also apply to the Ombudsman for permission not to comply with a request to stop or restrict processing. If so, you must do so within twenty-one days from the date of the request, and inform the individual that you have applied to the Ombudsman.

Do you have to tell other organisations about ceasing or restricting processing of personal data following a request from an individual?

If the Ombudsman issues an order to block, erase or destroy data, she may if it is considered practicable order you to notify third parties to whom the data may have been disclosed of the blocking, erasure or destruction.

In any event, it is good practice to let any third parties to whom the personal data was disclosed know of the fact that you stop or restrict processing.

The DPA defines a third party as follows:

“third party”, in relation to personal data, means any person other than -
(a) the data subject;
(b) the data controller; or
(c) any data processor or other person authorised to process data for the data controller or data processor.

Can you refuse to comply with a request to cease or restrict processing?

If you do not wish to comply with a request to cease or restrict processing you can apply to the Ombudsman within twenty-one days from the date of the request.

If you apply to the Ombudsman you need to inform the individual that you did so.

As explained above, the right to demand that processing is stopped or restricted does not apply in all circumstances.

There are also certain exemptions from the right to stop or restrict processing.

⁶² See more on exemptions [here](#).

What are the exemptions to the right to stop or restrict processing?

Apart from the general circumstances when the right to stop or restrict processing does not apply, namely where the data is being processed in the context of a contract, a legal obligation or to protect the vital interests of the individual, the DPA recognizes the following exemptions from the right to stop or restrict processing:

- Section 18: exemption relating to national security;
- Section 22: exemption relating to journalism, literature and art;
- Section 24: exemption relating to information available to the public by law;
- Section 25: exemption relating to disclosure required by law or made in connection with legal proceedings; and
- Section 26: exemption relating to personal, family and household affairs.

How do you recognize a request to stop or restrict processing?

The DPA does not specify how to make a valid request, except to say that it must be made in writing.

A request can be made to any part of your organisation and does not have to be to a specific person or contact point. You may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request

A request does not have to include the phrase 'request for restriction' or section 10 of the DPA, as long as it is in writing and asks that data processing is stopped, not begun or that processing cease for a specified purpose or in a specified way

Additionally, it is good practice to have a policy for recording details of the requests you receive. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Can you charge a fee for responding to a request to stop or restrict processing?

You cannot charge a fee to comply with a request for stopping or restricting processing personal data.

How long do you have to comply with a request to stop or restrict processing?

The DPA does not set a timeline for your response to an individual's request to cease or restrict processing under section 10. However, section 6(1) of the Data Protection Regulations, 2018, allows a period of twenty-one days from the date of the request, for you to apply to the Ombudsman not to comply with a request to cease or restrict processing. Therefore, in effect, a response to the request to cease or restrict processing should also be provided within twenty-one days.

Can you ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Relevant provisions

Data Protection Act (2021 Revision):⁶³

Section 10:	Right to stop processing
Section 14:	Rectification, blocking, erasure or destruction
Section 43:	Complaints to the Ombudsman
Section 45:	Enforcement orders

Data Protection Regulations, 2018:⁶⁴

Regulation 6	Circumstances when data controller is not obliged to comply
--------------	---

⁶³ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁶⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

The right to stop direct marketing

At a glance

- The DPA gives individuals an absolute right to stop the processing of their personal data for direct marketing purposes.
- An individual must notify you in writing.
- When notified, you should cease, or not begin processing for the purpose of direct marketing without undue delay within a reasonable period of time.
- An individual may complain to the Ombudsman if you do not comply with their request.

Checklist

Preparing for objections to processing

- ☐ We know how to recognize a notice to stop direct marketing and we understand when the right applies.
- ☐ We have a policy in place for how to record objections we receive.
- ☐ We understand that it is best practice to inform individuals of their right to object to direct marketing, in addition to including it in our privacy notice.

Complying with requests which object to processing

- ☐ We have processes in place to ensure that we respond to a notification to stop direct marketing without undue delay within a reasonable period of time.
- ☐ We have appropriate methods in place to erase, suppress or otherwise cease processing personal data

In brief

- [What is “direct marketing”?](#)
- [The right to stop direct marketing](#)
- [Do you need to tell individuals about the right to stop direct marketing?](#)
- [Do you always need to erase personal data to comply with a notice to stop direct marketing?](#)
- [Can you refuse to comply with a notice to stop direct marketing?](#)
- [How do you recognize a notice to stop direct marketing?](#)
- [Can you charge a fee for responding to a notice to stop direct marketing?](#)
- [How long do you have to respond to a notice to stop direct marketing?](#)

- [Can you extend the time for a response to a notice to stop direct marketing?](#)
- [Can you ask an individual for ID before responding to a notice to stop direct marketing?](#)

What is “direct marketing”?

Section 11 of the DPA defines “direct marketing” as:

the communication, by whatever means, of any advertising, marketing, promotional or similar material, that is directed to particular individuals.

This does not cover general advertising as long as it is not directed at particular individual.

The right to stop direct marketing

An individual can ask you to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing, you must stop processing the individual’s data for this purpose.

This does not automatically mean that you need to erase the individual’s personal data, since you may be using it for other purposes. However, if you do not process the data for any other fair and legal purpose, you would need to erase the data.

Do you need to tell individuals about the right to stop direct marketing?

It is best practice to give individuals a choice to stop direct marketing at the time of your first communication with them. You should let them know:

- who you are;
- what the legal basis is of your processing; and
- how they can notify you that they no longer want you to process their data for direct marketing.

You should present this information clearly and separately from any other information.

Do you always need to erase personal data to comply with a notice to stop direct marketing?

If you only hold the data for direct marketing, and not for any other purpose, you must cease all processing of the individual's personal data and erase their data. The individual's right to demand that processing for direct marketing is absolute and cannot be denied.

You can use a suppression list to list the individuals that should not be contacted for direct marketing.

However, if you process the individual's personal data for any other purposes, you can continue to retain the data, as long as you meet all the other requirements of the DPA, including upfront notification of the purpose(s) for processing.

Example

An individual is contacted by email by their bank about a new personal finances service being introduced to long-time customers. The individual notifies the bank that they want direct marketing to stop within two weeks.

The bank must stop their direct marketing towards this individual, even though it may be a processing activity that is a "compatible purpose" under the second data protection principle. However, the bank can continue to process the individual's personal data for other banking purposes, as documented in the agreement between the bank and its customer, and communicated in the privacy notice.

Remember that the definition of "processing" under the DPA is very broad and includes holding and destroying data.

Can you refuse to comply with a notice to stop direct marketing?

No, you cannot refuse to comply with an individual's notice to stop direct marketing towards them.

How do you recognize a notice to stop direct marketing?

The DPA specifies that a notification to stop direct marketing must be in writing, but the individual does not have to use a particular form, mention section 11 of the DPA.

This may present a challenge as any of your employees could receive a valid notification. You should consider which of your staff who regularly interact with individuals may need specific training to identify a notice to stop processing for direct marketing purposes.

Additionally, it is good practice to have a policy for recording details of the objections you receive. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the notification. We recommend that you keep a log of all requests relating to data protection.

Can you charge a fee for responding to a notice to stop direct marketing?

No, there is no fee for a notice to stop direct marketing.

How long do you have to respond to a notice to stop direct marketing?

An individual who notifies you they want you to stop direct marketing towards them should give you a “reasonable period in the circumstances” to cease (or not begin) processing for the purposes of direct marketing.

If an individual does not give you a timeline for complying with their notification, you should stop the processing without undue delay.

Can you extend the time for a response to a notice to stop direct marketing?

No, there is no extension of the time period for stopping to process personal data for direct marketing. If you find that the period indicated in the notification is not reasonable, you can contact the Ombudsman and provide her with any reasons for delay.

Can you ask an individual for ID before responding to a notice to stop direct marketing?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Relevant provisions

Data Protection Act (2021 Revision):⁶⁵

Section 11:

Right to stop processing for direct marketing

Further guidance

DMA guidance for marketers

<https://dma.org.uk/article/dma-gdpr-guidance-for-marketers>

⁶⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Rights in relation to automated decision making

At a glance

- The DPA has provisions on solely automated individual decision-making (making a decision exclusively by automated means without any human involvement).
- An individual may at any time give you a notice in writing requiring that a decision which affects significantly them is not solely based on processing by automated means.
- If you make decisions that significantly affect individuals solely by automated means, you must notify the individual that the decision was taken on that basis.
- The individual may then notify you within twenty-one days that you need to reconsider the decision on a different basis (not solely based on automated means). You must then, within twenty-one days inform the individual explaining what steps you intend to take to comply with the notice.
- This right is not absolute and there are circumstances when it does not apply.

Checklist

All automated individual decision-making and profiling

To comply with the DPA

- ☐ We meet a lawful condition in Schedule 2 of the DPA to carry out automated decision-making.
- ☐ We provide individuals with a privacy notice when obtain their personal data indirectly.
- ☐ We only collect the minimum amount of data needed and have a clear retention policy for the data we use for the automated decisions we take about individuals.
- ☐ We tell our customers about the automated decision-making we carry out which impact them significantly.
- ☐ We respond within twenty-one days to notifications received from individuals requiring us to reconsider the decision or make a new decision on a different (non-automated) basis, by specifying what steps we intend to take to meet their notification.

As a model of best practice

- ☐ We have additional checks in place for our automated decision-making systems to protect any vulnerable groups (including children).

- ☐ We carry out a privacy impact assessment to consider and address the risks before we start any new automated decision-making.
- ☐ We inform individuals what information we use to make solely automated decisions, and where we get this information from.
- ☐ We use anonymized data in our solely automated individual decision-making.
- ☐ We don't use sensitive personal data in our automated decision-making systems unless that processing meets one of the conditions Schedule 3 of the DPA.
- ☐ We have a simple way for people to ask us to reconsider an automated decision.
- ☐ We have identified staff in our organisation who are authorised to carry out reviews and change decisions.
- ☐ We regularly check our systems for accuracy and bias and feed any changes back into the design process.

In brief

- [What is automated individual decision-making?](#)
- [What does the DPA say about automated individual decision-making?](#)
- [What do you need to do under the DPA?](#)
- [Are there circumstances when you do not need to comply with an individual's notice relating to automated processing?](#)
- [What else do you need to consider?](#)
- [Can you charge a fee for responding to a notice to stop automated decision making?](#)
- [How long do you have to respond to a notice relating to automated decision making?](#)
- [Can you extend the time for a response to a notice relating to automated decision making?](#)
- [Can you ask an individual for ID before responding to a notice relating to automated decision making?](#)

What is automated individual decision-making?

The DPA does not define automated decision making, but it means a decision made by automated means without any human involvement.

Examples of this include:

- creditworthiness, e.g. in a decision relating to a bank loan;
- the individual's performance at work; or a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, but it often will do.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But they can also represent significant risks for individuals. Section 12 of the DPA is designed to address these risks.

What does the DPA say about automated individual decision-making?

The DPA restricts you from making solely automated decisions, including those based on profiling, that have a significant effect on individuals.

Individuals have the right to require – at any time - that decisions which affect them substantially are taken on a different basis than a solely automated basis.

For something to be solely automated there must be no human involvement in the decision-making process. A decision with a mere token human involvement, such as where a human simply takes over the automated decision without any substantive appraisal, will still be deemed to be automated for purposes of the DPA.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the DPA, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is, for instance, something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

What do you need to do under the DPA?

If you engage in solely automated individual decision-making with significant effects on an individual, you must:

- notify the individual as soon as practicable; and
- allow the individual within twenty-one days to require that the decision is reconsidered or that a new decision is taken on a different basis.

Within twenty-one days from receiving the individual's notice, you must then inform the individual in writing of the steps you are taking to comply with their notice.

Are there circumstances when you do not need to comply with an individual's notice relating to automated processing?

An individual's notice to require you to reconsider or redo a decision that was taken solely on an automated basis does not apply if one each of the following listings of conditions is met:

1. the decision is taken in the course of:
 - (a) considering whether to enter into a contract with the individual
 - (b) entering into such a contract, or
 - (c) performing such a contract.and,
2. (a) the decision grants a request from the individual; or
(b) steps have been taken to safeguard the legitimate interests of the individual including allowing the individual to make representations.

Example

An individual applies for a loan with their bank. The bank uses automated decision-making to evaluate the customer's credit worthiness.

Where the loan is approved, the exemption applies, as the decision met two of the required conditions, namely being taken in the course of considering whether to enter into a contract with the individual (1a), and granting a request (the loan) from the individual (2a).

Where the loan is denied, the exemption will only apply where the second condition, 2b), is met. This may be that the logic of the decision is explained to the individual and an avenue is provided for the individual to challenge the decision and have it re-evaluated.

What else do you need to consider?

You should be able to:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
 - obtain human intervention;
 - express their point of view; and
 - obtain an explanation of the decision and challenge it;

- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimize the risk of errors; and
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

Can you charge a fee for responding to a notice to stop automated decision making?

There is no fee for a notice to reconsider or remake a decision on a different basis than a solely automated basis.

How long do you have to respond to a notice relating to automated decision making?

When an individual notifies you that they require that a decision solely made on an automated basis must be reconsidered or remade, you have twenty-one days to let them know what steps you are taking to comply with their notice.

Can you extend the time for a response to a notice relating to automated decision making?

No, there is no extension of the twenty-one day time period for letting an individual know what steps you are taking to comply with their notice relating to automated decision making.

Can you ask an individual for ID before responding to a notice relating to automated decision making?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay if you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Relevant provisions

Data Protection Act (2021 Revision):⁶⁶

Section 12: Rights in relation to automated decision making

Further guidance

ICO: Guidance on automated decision making and profiling⁶⁷
Article 29 Working Party: Guidelines on automated individual decision making and profiling⁶⁸

⁶⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁶⁷ <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/>

⁶⁸ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

The right to complain / seek compensation

At a glance

- An individual has the right to complain to the Ombudsman about any perceived violation of the DPA.
- The Ombudsman may also investigate matters under the DPA on her own motion.
- An individual suffers damage due to a contravention of the DPA by a data controller may seek compensation in the courts.

In brief:

- [Who can complain to the Ombudsman?](#)
- [What can an individual complain about to the Ombudsman?](#)
- [Will the Ombudsman automatically investigate a complaint?](#)
- [How will the Ombudsman handle offences?](#)

Who can complain to the Ombudsman?

An individual can complain on their own or someone else's behalf.

If someone complains on behalf of another, they must provide written authorisation from the aggrieved person.

What can an individual complain about to the Ombudsman?

A complaint to the Ombudsman under the DPA has to relate to personal data processing that has not been or is not being carried out in compliance with the provisions of the DPA, or anything done pursuant to the DPA.

The complaint does not have to relate to the processing of the personal data of complainants themselves.

However, if someone is complaining on behalf of another, the complaint must relate to the processing of the personal data of the person on whose behalf the complaint is being made ("the aggrieved person").

Will the Ombudsman automatically investigate a complaint?

The Ombudsman may investigate a complaint under the DPA or start an investigation on her own motion.

The Ombudsman may determine whether to conduct an investigation, or not, on the basis of (including):

- the extent to which the complaint appears to raise a matter of substance;
- any undue delay in making the complaint;
- whether the complaint is frivolous or vexatious; and
- whether the person making the complaint is entitled to make a subject access request under section 8.

How will the Ombudsman handle offences?

The Ombudsman will refer alleged offences to the Director of Public Prosecution for possible prosecution in the courts.

Relevant provisions

Data Protection Act (2021 Revision):⁶⁹

Section 43: Right to complain to the Ombudsman

Section 13: Compensation for failure to comply

⁶⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Personal data breaches

At a glance

- The DPA introduces a duty on all data controllers to report personal data breaches to the Ombudsman and the individual(s) whose data was breached, unless the breach is unlikely to prejudice their rights and freedoms. You must do this within 5 days.
- You need to provide the Ombudsman and the individual(s) with certain information, including measures you have taken, and measures you recommend the individual to take.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate your communications with the Ombudsman and the individuals.

Checklist

Preparing for a personal data breach

- ☐ We know how to recognize a personal data breach.
- ☐ We understand that a personal data breach is not only about loss or theft of personal data.
- ☐ We have prepared a response plan for addressing any personal data breaches that occur.
- ☐ We have allocated responsibility for managing breaches to a dedicated person or team.
- ☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- ☐ We have in place a process to assess the likely risks to individuals as a result of a breach.
- ☐ We know the Ombudsman is the relevant supervisory authority for our processing activities.
- ☐ We have a process to notify the Ombudsman and the affected individuals of a breach within 5 days, even if we do not have all the details yet.
- ☐ We know what information we must give the Ombudsman and the individuals about a breach.
- ☐ We know what information about a breach we must provide to the Ombudsman and affected individuals, including advice to help them protect themselves from its effects.

In brief

- [What is a personal data breach?](#)
- [What breaches do you need to notify the Ombudsman and affected individuals about?](#)
- [What role do processors have?](#)
- [How much time do you have to report a breach?](#)
- [What information must a breach notification to the Ombudsman and the affected individuals contain?](#)
- [What if we don't have all the required information available yet?](#)
- [How do you notify a breach to the ICO?](#)
- [Are there any breaches I do not need tell the affected individuals about?](#)
- [Does the DPA require you to take any other steps in response to a breach?](#)
- [What happens if you fail to notify?](#)

What is a personal data breach?

The DPA defines a “personal data breach” as follows:

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or, access to, personal data transmitted, stored or otherwise processed.

Breaches can be the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a (security) incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on

without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed due to a malfunction of the storage medium.

When a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the Ombudsman and the individuals that may be affected if there are likely risks that to the rights and freedoms of the individuals affected.

What breaches do you need to notify the Ombudsman and affected individuals about?

The Ombudsman expects all data breaches to be reported to the Ombudsman and the individual(s) whose data was breached.

A personal data breach may not by itself lead to enforcement action by the Ombudsman. The circumstances of the breach will determine whether an investigation will be launched. A breach notification form can be found on the website of the Ombudsman.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

What role do processors have?

If your organisation uses a data processor, and this data processor suffers a reportable breach, then you – as the data controller - must inform the Ombudsman, and the individual(s) concerned, without undue delay and always within the five-day reporting time limit.

Example

Your organisation (the data controller) contracts an IT services firm (the data processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the Ombudsman and the individual(s) concerned.

If you use a data processor, the requirements on breach reporting should be detailed in the contract between you and your data processor, as required under the [seventh data protection principle](#) and paragraph 3 of part 2 of Schedule 1.

How much time do you have to report a breach?

You must report a personal data breach to the Ombudsman and the individual(s) concerned without undue delay, but not later than 5 days after you should, with the exercise of due diligence, have been aware of the breach.

In the context of data breaches, due diligence means that you must manage your systems on an ongoing basis and monitor them for any accidental or deliberate destruction, loss, alteration, unauthorised disclosure of or, access to, the personal data you process.

What information must a breach notification to the Ombudsman and the affected individuals contain?

When reporting a breach, the DPA says you must provide a description of:

- the nature of the personal data breach;
- the consequences of the breach;
- the measures proposed or taken by yourself to address the breach; and
- the measures you recommend the individual(s) to take to mitigate the possible adverse effects of the breach.

What if we don't have all the required information available yet?

Data controller are expected to prioritize the investigation, give it adequate resources, and expedite it urgently. Nonetheless, it may not always be possible to investigate a breach fully within 5 days to understand exactly what has happened and what needs to be done to mitigate it.

If so, you should provide the additional information as soon as possible without undue further delay.

If you cannot provide full details within 5 days, it is a good idea to explain the delay to the Ombudsman and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the Ombudsman and individuals within 5 days of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the Ombudsman and the individuals more information about the breach without delay.

How do you notify a breach to the Ombudsman?

To notify the Office of the Ombudsman of a personal data breach, please see the contact page on our website: <http://ombudsman.ky/get-in-touch>.

Are there any breaches I do not need tell the affected individuals about?

The DPA requires that all personal data breaches are reported to both the Ombudsman and the affected individuals within 5 days.

Example

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms. This breach must be reported to the Ombudsman and the individuals concerned.

A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a risk to the rights and freedoms of those individuals. This breach does not need to be reported to the Ombudsman and the individuals concerned.

Does the DPA require you to take any other steps in response to a breach?

It is best practice to record all breaches.

As with any security incident, you should investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What happens if you fail to notify?

Not notifying a breach in time may cause additional damages to the individual's whose data has been breached. This will damage your reputation and undermine the trust individuals have in your business or organisation.

Failing to notify a breach when required to do so is an offence under the DPA and can result in a conviction and a fine of one hundred thousand dollars.

Failing to notify may also be subject to a monetary penalty imposed by the Ombudsman under section 55 of the DPA.

Relevant provisions

Data Protection Act (2021 Revision):⁷⁰

Section 16: Personal data breaches

Further guidance

Article 29 Working Party: Guidelines on personal data breach notification⁷¹

⁷⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁷¹ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Exemptions

The DPA exempts the processing of certain personal data from specified parts of the Act. All other provisions of the DPA outside the specified exemption continue to apply.

National security

What is exempted?

This exemption applies to the processing of personal data for national security purposes.

What provisions in the DPA does the exemption relate to?

Under this exemption, personal data is exempt from:

- all the data protection principles;
- Part 2 (the rights of individuals);
- Part 3 (personal data breach notification); and
- Part 6 (enforcement by the Ombudsman).

When does the exemption apply?

The exemption from all or any of the provisions applies to the extent required to safeguard national security.

How does the exemption work?

The Governor has the discretion to issue a certificate relating to any personal data, exempting it from all or any of the provisions above.

The Governor may consult with the National Security Council on the issuing of the certificate.

The Governor's certificate identifies the personal data it relates to.

When a data controller claims that a certificate by the Governor applies to personal data being considered by the Ombudsman, any party (the Governor, the data controller or the data subject) may contend that the certificate does not apply to the personal data in question.

The Ombudsman may make a determination whether the certificate applies or does not apply to the personal data in question.

Relevant provisions

Data Protection Act (2021 Revision):⁷²

Section 18:

Exemption relating to national security

⁷² https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Crime, government fees and duties

What is exempted?

1. This exemption applies to personal data processed for:
 - the prevention, detection, or investigation of crime;
 - the apprehension or prosecution of persons suspected of having committed an offence (anywhere); or
 - the assessment or collection of any fees or duties, or impositions of a similar nature (in the Cayman Islands).
2. Personal data processed for the discharging of functions under any law and that consists of information obtained from someone who had possession of it for the above purposes is also covered.

What provisions in the DPA does the exemption relate to?

1. The first part of the exemption applies to:
 - the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required);
 - the second data protection principle (purpose limitation);
 - the third data protection principle (data minimization);
 - section 8 (the access right);
 - section 10 (the right to stop or restrict processing); and
 - section 14 (the right to rectification).
2. The second part of the exemption applies to:
 - the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); and
 - section 8 (the access right).

When does the exemption apply?

The exemption does not automatically apply to all information relating to crime and government fees.

The exemption applies to the extent the application of those provisions would be likely to prejudice the matters listed (crime and government fees).

Relevant provisions

Data Protection Act (2021 Revision):⁷³

Section 19:

Exemption relating to crime, government fees and duties

⁷³ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Health

What is exempted?

This exemption applies to personal data the release of which could reasonably cause mental or physical harm to the data subject or any other person.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from the subject information provisions, i.e.:

- the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); and
- section 8 (the access right).

When does the exemption apply?

Only personal data that can reasonably be expected to cause mental or physical harm to an individual, if disclosed, is covered by this exemption.

That individual can be the data subject or any other individual.

How does this exemption work?

If you as the data controller are not a health professional, the exemption applies if:

- at the time of a request for access you consult with the appropriate health professional on the question whether the exemption applies and you obtain a written opinion that the exemption applies to the data; or
- you consulted with the appropriate health professional beforehand and obtained a written opinion that the exemption applies to the data.

The health professional's opinion must be no older than six months when the request is made.

Even if the opinion was obtained within the last six months, it may be reasonable considering all circumstances to consult the appropriate health professional again.

The DPA does not define an “appropriate” health professional, but it is assumed this means a health professional who can issue a professional opinion on the mental or physical harm that would likely be done by making the information accessible to the individual.

The DPA defines a “health professional” as follows:

“health professional” means an individual registered to practice under any of the professions specified in the Health Practice Act (2021 Revision) or any other Act relating to health;

A “health record” is defined as:

“health record” means a record that –

- (a) consists of information relating to the physical health, mental health or condition of a data subject; and
- (b) has been made by or on behalf of a health professional in connection with the care of that data subject;

Relevant provisions

Data Protection Act (2021 Revision):⁷⁴

Section 20:	Exemption relating to health, education or social work
-------------	--

Data Protection Regulations, 2018:⁷⁵

Regulation 7	Exemption relating to health
--------------	------------------------------

⁷⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁷⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

Education

What is exempted?

This exemption applies to an educational record if its disclosure to the data subject would be likely to cause serious harm to the physical or mental health or condition of that individual or any other person.

An educational record includes information about whether the data subject who is a child is or has been subject to abuse, or may be at risk of it.

An educational record also includes an exam or test question that is likely to be used within the next twelve months.

“Abuse” in relation to a child:

- (a) includes physical injury to and physical neglect, emotional neglect, ill-treatment and sexual abuse of the person; and
- (b) excludes accidental injury.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- section 8 (the access right).

When does the exemption apply?

The personal data must be an educational record and its disclosure must be likely to cause serious harm to the mental or physical health or condition of an individual.

What else is there to consider?

If the request for access is made by a parent or a legal guardian (appointed by the court to manage the affairs of the child) on behalf of the child, personal data relating to actual or potential abuse of the child

is exempt from section 8 (the right to access), but only to the extent that disclosure would not be in the interests of the child.

Relevant provisions

Data Protection Act (2021 Revision):⁷⁶

Section 20:	Exemption relating to health, education or social work
-------------	--

Data Protection Regulations, 2018:⁷⁷

Regulation 8	Exemption relating to education
--------------	---------------------------------

⁷⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁷⁷ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

Social Work

What is exempted?

This exemption potentially applies to a very wide range of personal data processing.

This exemption applies to personal data in relation to:

- social work;
- allocation of housing or other residential accommodation;
- benefits under the Health Insurance Act (2021 Revision);
- benefits under the Poor Persons (Relief) Act (1997 Revision);
- probation;
- school attendance;
- ensuring children receive suitable education;
- guardianship under the Grand Court Act (2015 Revision);
- any function under the Children Act (2012 Revision);
- any function under the Adoption of Children Act (2021 Revision);
- any function under the Mental Health Act (2021 Revision);
- any function under the Older Persons Act (2021 Revision); and
- any other applicable law.

The exemption also applies to personal data processed by a court, supplied to the court as evidence in proceedings relating to families or children, which the court:

- considers impracticable to disclose having regard to the data subject's age and understanding; or
- considers undesirable to disclose because serious harm might be suffered by the data subject by the disclosure.

In the context of this exemption, the term "proceedings relating to families or children" includes proceedings relating to adoption, matrimonial matters and guardianship.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); and
- section 8 (the access right).

When does the exemption apply?

The exemption applies to the extent that the application of these provisions would be likely to prejudice the carrying out of social work because they would cause serious harm to the physical or mental health or condition of the data subject or any other individual.

What else is there to consider?

Where a parent or guardian appointed by the court exercises the right to access on behalf of a data subject, the information is exempt from the right to access in section 8 of the DPA to the extent that it would result in disclosing information:

- provided by the data subject in the expectation that it would not be disclosed to the parent or guardian making the request;
- obtained during an examination or investigation in the expectation that the information would not be so disclosed; or
- that the data subject has expressly indicated should not be so disclosed.

The above applies, unless the data subject has expressly indicated that it no longer expects that the information would not be disclosed.

Relevant provisions

Data Protection Act (2021 Revision):⁷⁸

Section 20:	Exemption relating to health, education or social work
-------------	--

Data Protection Regulations, 2018:⁷⁹

Regulation 9	Exemption relating to social work
--------------	-----------------------------------

⁷⁸ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

⁷⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Regulations_2018.pdf

Monitoring, inspection or regulatory function

What is exempted?

This exemption applies to personal data that is processed for the purpose of any monitoring, inspection or regulatory function connected with the exercise of a public function in relation to:

- public safety;
- prevention, investigation, detection and prosecution of criminal offences;
- prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- an important economic or financial interest of the Cayman Islands, including:
 - compliance with international tax treaties or international cooperation;
 - any monitoring, inspection or regulatory function exercised by official authorities (including regulation of the financial services industry); and
 - any monetary, budgetary and taxation purposes in the Cayman Islands.
- a public function conferred on any person under any law or regulations;
- a function of the Crown, the Governor in Cabinet or a public authority; and
- any other function of a public nature.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- the subject information provisions insofar as they would likely prejudice the monitoring, inspection or regulatory functions.

When does the exemption apply?

The exemption applies to the extent that the application of these provisions would be likely to prejudice the proper discharge of the function.

Relevant provisions

Data Protection Act (2021 Revision):⁸⁰

Section 21: Exemption relating to monitoring, inspection or regulatory functions

⁸⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Journalism, literature or art

What is exempted?

The exemption applies to personal data processed only for the special processes. These are defined as:

- journalism;
- artistic purposes; and
- literary purposes.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- the data protection principles except the seventh data protection principle (security – integrity and security); and
- section 10 (the right to stop processing).

When does the exemption apply?

For the exemption to apply, processing must:

- be undertaken with a view to the publication of journalistic, artistic or literary materials;
- the data controller must reasonable believe publication would be in the public interest (having regard to the particular importance of freedom of expression); and
- the data controller must believe compliance with the exempted provision is incompatible with the special purpose.

What else is there to consider?

In considering whether it is reasonable to consider that the processing is in the public interest, regard may be had to any code of practice that is relevant to the publication, which the data controller has complied with.

Relevant provisions

Data Protection Act (2021 Revision):⁸¹

Section 4:	Definition of special purposes
Section 22:	Exemption relating to journalist, literature and art

⁸¹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Research, history or statistics

What is exempted?

This exemption relates to personal data processes for the purposes of research (understood to be scientific research and not e.g. marketing research), history or statistics.

The exemption may apply only if:

- the personal data is not processed to support a measure or decision relating to a particular individual; and
- the personal data is not processed in a way that likely causes substantial damage or substantial distress to any individual.

What provisions in the DPA does the exemption relate to?

1. Under this exemption personal data is exempt from the first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 (notification of the purpose for the processing).
2. Personal data processed only for scientific research purpose, or which is kept in a form that identifies a data subject only for as long as required to create statistics, is exempt from section 8 of the DPA (the right to access).
3. Personal data processed for historical, statistical or scientific purposes is exempt from the fifth data protection principle (storage limitation) to the extent that compliance would be likely to prejudice those purposes.

When does the exemption apply?

1. The exemption (from the first data protection principle) applies if the provision of the notification of the purpose would prove impossible or would involve a disproportionate effort.

The exemption also applies if the processing is required by law

2. The exemption (from section 8 of the DPA) applies if:
 - the data is processed in compliance with the relevant conditions;

- there is no risk of breaching the rights and freedoms of the data subject; and
 - the results of the research or resulting statistics does not identify one or more data subject.
3. The exemption from the fifth data protection principle applies to the extent that complying would prejudice the historical, statistical or scientific research.

What else is there to consider?

Processing for the purposes of scientific research, history or statistics does not constitute “incompatible processing” under the second data protection principle.

Relevant provisions

Data Protection Act (2021 Revision):⁸²

Section 23:

Exemption relating to research, history or statistics

⁸² https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Information available to public by or under enactments

What is exempted?

This exemption applies to personal data which the data controller is obliged to make available to the public by law, including by means of inspection, whether free of charge or for payment of a fee.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required);
- the second data protection principle (purpose limitation principle);
- the third data protection principle (data minimization principle);
- the fourth data protection principle (data accuracy principle);
- section 8 (the access right);
- section 10 (right to stop or restrict processing)
- section 14 (rectification, blocking, erasure or destruction)

When does the exemption apply?

The exemption applies whenever the personal data is required to be made public by or under an enactment.

Relevant provisions

Data Protection Act (2021 Revision):⁸³

Section 24

Exemption relating to information available to the public
by law

⁸³ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Disclosures required by law or made in connection with legal proceedings

What is exempted?

This exemption applies to personal data that is required to be disclosed under any enactment, by any law or by a court order.

The exemption also applies where the disclosure of the personal data is necessary:

- for, in connection with or in contemplation of any quasi-judicial or legal proceedings;
- for the purpose of obtaining legal advice;
- otherwise for the purposes of establishing, exercising or defending a legal right.

What provisions in the DPA does the exemption relate to?

Under this exemption personal data is exempt from:

- the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required);
- the second data protection principle (purpose limitation principle);
- the third data protection principle (data minimization principle);
- section 10 (the right to stop or restrict processing); and
- section 14 (the right to rectification).

When does the exemption apply?

The exemption applies to the extent that the listed provisions are inconsistent with the disclosure in question.

Relevant provisions

Data Protection Act (2021 Revision):⁸⁴

Section 25:

Exemption relating to disclosures required by law or in connection with legal proceedings

⁸⁴ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Personal, family or household affairs

What is exempted?

This exemption applies to personal data processed by an individual only for the purposes of that individual's personal, family or household affairs. The scope of the exemption is very narrow, like all exemptions. Any use of personal data by an organisation of any type will not fall under this exemption. The publication of information will also not fall under this exemption.

What provisions in the DPA does the exemption relate to?

Under this exemption the personal data are exempt from:

- all data protection principles;
- Part 2 (rights of individuals); and
- Part 3 (personal data breach notification).

Relevant provisions

Data Protection Act (2021 Revision):⁸⁵

Section 26:	Exemption relating to personal, family or household affairs
-------------	---

⁸⁵ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Honours

What is caught by this exemption?

This exemption applies to personal data that is processed by the Crown or the Premier for the purposes of conferring any honour or dignity.

What provisions in the DPA does the exemption relate to?

Under this exemption the personal data is exempt from:

- the first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 (notification of the purpose for the processing); and
- section 8 (the access right).

Relevant provisions

Data Protection Act (2021 Revision):⁸⁶

Section 27:

Exemption relating to honours

⁸⁶ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Corporate finance

What is exempted?

This exemption applies to personal data processed for the purposes of a corporate finance service provided by:

- a legally registered person providing for investment business;
- a person who is exempted from the obligation to be legally registered to provide an investment business;
- a person who is an authorised person providing for investment business;
- a person who is exempt in respect of investment business;
- a person who through their employment offers a corporate finance service; or
- a partner who provides a corporate finance service in a partnership.

“Corporate finance service” is defined as a service consisting of:

- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
- (b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
- (c) services relating to such underwriting as mentioned in paragraph (a)

What provisions in the DPA does the exemption relate to?

Under this exemption the personal data is exempt from:

- the first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 (notification of the purpose for the processing); and
- section 8 (the access right).

When does the exemption apply?

The personal data is exempt to the extent that:

- the application of the provisions to the data could affect the price of any instrument; or

- the data controller believes the application of the provisions to the data could affect the price of an instrument.

The personal data may also be exempt if the exemption is necessary to safeguard an important economic or financial interest of the Cayman Islands.

What else is there to consider?

For the purposes of this exemption an “instrument” represents investment, and may already be in existence, may be, or may yet to be created.

Relevant provisions

Data Protection Act (2021 Revision):⁸⁷

Section 28:

Exemption relating to corporate finance

⁸⁷ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Negotiations

What is exempted?

This exemption applies to personal data that consists of a record of the intentions of the data controller in relation to any negotiations with the data subject.

What provisions in the DPA does the exemption relate to?

Under this exemption the personal data is exempt from:

- the first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 (notification of the purpose for the processing); and
- section 8 (the access right).

When does the exemption apply?

The exemption applies to the extent that the application of the provisions would be likely to prejudice the negotiations.

Relevant provisions

Data Protection Act (2021 Revision):⁸⁸

Section 29:

Exemption relating to negotiations

⁸⁸ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Legal professional privilege and trusts

What is exempted?

This exemption applies to personal data which consists of information:

1. which is subject to legal professional privilege; or
2. in relation to any structure or arrangement that is an ordinary trust, any structure or arrangement that is a trust established under the Trusts Act (2021 Revision), or any will made pursuant to the Wills Act (2021 Revision).

What provisions in the DPA does the exemption relate to?

Under this exemption the personal data is exempt from:

- the first data protection principle to the extent that it requires compliance with paragraph 2 of Part 2 of Schedule 1 (notification of the purpose for the processing); and
- section 8 (the access right).

Relevant provisions

Data Protection Act (2021 Revision):⁸⁹

Section 30:

Exemption relating to legal professional privilege and trusts

⁸⁹ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Contracts between data controllers and data processors

At a glance

- Whenever a data controller uses a data processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- Data controllers remain liable for their compliance with the DPA even if the processing of personal data is delegated.
- Data processors must only act on the documented instructions of a controller. Data processors which breach their contractual obligations may be liable for damages to the affected data controller. The Ombudsman has certain investigatory powers, non-compliance with which may lead to prosecution.

Checklist

Contracts must include the following mandatory terms:

- ☐ the data processor must only act on the written instructions of the data controller (unless required by law to act without such instructions);
- ☐ the data processor must take appropriate measures to ensure the security of processing.

Contracts should, as a matter of good practice, include the following details:

- ☐ the subject matter and duration of the processing;
- ☐ the nature and purpose of the processing;
- ☐ the type of personal data and categories of data subject; and
- ☐ the obligations and rights of the controller.

Contracts should include the following terms:

- ☐ the data processor must ensure that people processing the data are subject to a duty of confidence;
- ☐ the data processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- ☐ the data processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the DPA;
- ☐ the data processor must assist the data controller in meeting its DPA obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

- ☐ the data processor must delete or return all personal data to the controller as requested at the end of the contract; and
- ☐ the data processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their legal obligations, and tell the controller immediately if it is asked to do something infringing the DPA.

As a matter of good practice, our contracts:

- ☐ state that nothing within the contract relieves the data processor of its own direct responsibilities and liabilities under the DPA; and
- ☐ reflect any indemnity that has been agreed.

Checklist

In addition to the obligations set out in the checklist above, a data processor should practice the following best practices. The data processor must:

- ☐ co-operate with the Ombudsman in accordance with Part 6 of the DPA;
- ☐ ensure the security of its processing in accordance the [seventh data protection principle](#); and
- ☐ notify any [personal data breaches](#) to the controller in accordance with section 16 of the DPA.

A data processor should also be aware that:

- ☐ it may be subject to investigative and corrective powers of the Office of the Ombudsman under Part 6 of the DPA;
- ☐ if it fails to meet its obligations, the data controller may be subject to an administrative fine under section 55 of the DPA.

In brief

- [When is a contract needed?](#)
- [Why are contracts between data controllers and data processors important?](#)
- [What needs to be included in the contract?](#)
- [Can standard contracts clauses be used?](#)
- [What responsibilities and liabilities do data processors have in their own right?](#)

When is a contract needed?

Whenever a data controller uses a data processor (a recipient who processes personal data on behalf of the controller) it should have a written contract in place. Similarly, if a data processor employs another sub-data processor, it needs to have a written contract in place, as it will be a data controller towards that data processor.

Appropriate contractual measures will be an important aspect of assessing your compliance with the [seventh data protection principle](#) (security – integrity and security).

This obligation may overlap with your obligations under the [eighth data protection principle](#) (international transfers) where you transfer personal data outside the Cayman Islands.

What needs to be included in the contract?

Contracts must include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the data controller;
- take appropriate measures to ensure the security of processing.

Where the data processor has a limited need to use personal data for its own purposes (e.g. to comply with legal/regulatory requirements that apply to the data processor), this should be noted as an exception to the general rule that the data processor should only act on the data controller's instruction. In this case, the data processor will be a data controller in its own right, with all rights and obligations pursuant to the DPA.

Additionally, depending on the nature and scope of processing undertaken by the data processor and the risk posed, it might be appropriate to include additional requirements, for example those requiring the data processor to:

- ensure that all staff processing the data are subject to a duty of confidence;
- only engage sub-processors with the prior approval of the data controller and under a written contract;
- assist the data controller in providing subject access and allowing data subjects to exercise their rights under the DPA;
- assist the data controller in meeting its DPA obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the data controller as requested at the end of the contract; and

- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations under the DPA, and tell the data controller immediately if it is asked to do something infringing the DPA or other data protection law.

Where the processing undertaken by the data processor is particularly complex, or affects many different types of data subjects and/or personal data, it might be desirable for the contract to explain the specific context in which processing is performed, for example by specifying the subject matter and duration of the processing, the nature and purpose of the processing, and the type of personal data and categories of data subject.

We are aware that it may be difficult for some local data controllers to get larger organisations to amend their standard DPAs that reference EU law. The requirements under the DPA are also found in EU law. An EU compliant DPA will consequently also be compliant under the Cayman DPA.

What responsibilities and liabilities do data processors have in their own right?

A data processor must only act on the documented instructions of the data controller. If a data processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a data controller and will have the same liability as any data controller.

In addition to its contractual obligations to the data controller, a data processor must also comply with the [seventh data protection principle](#) (security – integrity and security), by ensuring that equivalent obligations as those imposed on the data controller are observed.

The data processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with the Office of the Ombudsman;
- to ensure the security of its processing;
- to document their processing activities; and
- to notify any personal data breaches to the data controller without delay.

If a data processor fails to meet any of these obligations or acts outside or against the instructions of the data controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a data processor uses a sub-processor then it will, as the original data processor, remain directly liable to the data controller for the performance of the sub-processor's obligations.

Relevant provisions

Data Protection Act (2021 Revision):⁹⁰

Schedule 1, Part 2, para 3:

Processing contract to ensure reliability

Part 6

Enforcement

⁹⁰ https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf

Questions or comments?

Please contact as at info@ombudsman.ky with any questions or comments.

Visit us on www.ombudsman.ky for further information about the Office of the Ombudsman.