Data Protection Policy

V2.0

Contents

1. Policy statement

1.1 We are committed to protecting the rights and privacy of individuals, tenants, employees, Non-Executive Board/Committee Members and other associated parties. We will do this in accordance with the General Data Protection Regulation and the Data Protection 2018, and any subsequent data protection legislation that applies to us.

1.2 We collect personal and special category data:

- to carry out our business functions and activities, and;
- to provide services to our tenants, employees, Non-Executive Board/Committee Members and other associated parties.

1.3 We will only collect and process personal data in compliance with the GDPR, the DPA 2018, and any subsequent protection legislation that applies to us.

1.4 We are registered with Information Commissioners Office ("**ICO**") and appear on the Data Protection Register as a controller of personal information. Our registration is renewed annually. Our ICO reference number is **Z6383822**.

2. Purpose

2.1 This policy outlines how we comply with the General Data Protection Regulation and the Data Protection 2018, and any subsequent data protection legislation that applies to us.

3. Scope

3.1 This policy applies to all our employees, tenants, Non-Executive Board/Committee Members, and any of our associated third parties.

3.2 In accordance with the DPA 2018 and Article 2(1) of the GDPR, this policy applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

See **Section 3.3** for definitions of '**automated means**', '**processing**', '**personal data**' and '**filing system**'.

3.3 Key definitions

3.3.1 The following terms are used in this policy, in accordance with the General Data Protection Regulation and Data Protection Act 2018:

Automated means	Refers to all information held on a computer or on other electronic systems. The processing of personal data "**other than by automated means**" refers to any information partly in paper, hard copy of other manual records.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data protection law	Refers to the General Data Protection Regulations (GDPR), the Data Protection Act (DPA) 2018, and any subsequent data protection legislation that applies to us.
Data subject	A data subject is any natural person whose personal data is being collected, held or processed, and can be identified directly or indirectly from that personal data.
DPA 2018	The Data Protection Act 2018.
Filing system	In accordance with the GDPR, a 'filing system' is "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".
GDPR	The General Data Protection Regulation.
Natural person or Living person	In accordance with the GDPR and DPA 2018, a 'natural person' or 'living person' refers to living human being. Therefore, information relating to a deceased person does not constitute personal data and is not subject to the GDPR or DPA 2018. Information about companies or public authorities does also not constitute personal data.
Near miss data breach	A near miss data breach is a data incident that did not result in the loss of personal data but had the potential to. See also 'Data breach'.
Process ***(-ed) (-ing)***	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or; destruction.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Personal data	Under Article 4(1) of the GDPR, personal data is defined as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
Special category data	Personal data which is identified as more sensitive under data protection law. This may include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included in this definition.

4. Responsibilities

4.1 Data controller

Where we are the controller of personal data, we are responsible for complying with the GDPR and DPA 2018. This involves implementing appropriate technical and organisational measures in an effective manner to ensure we comply with data protection law.

4.2 All employees and Non-Executive Board/Committee Members

All our employees and Non-Executive Board/Committee Members have a responsibility to process personal data in accordance with data protection law. All our employees and Non-Executive Board/Committee Members are responsible for ensuring that any personal data which they hold is kept securely and that they are not disclosed to any unauthorised third party. Any breach of this policy or related legislation, policies and procedures could be considered to be an offence and may result disciplinary proceedings.

4.3 All associated third parties

All of our associated third parties have a responsibility to process personal data in accordance with data protection law.

5. Data compliance and security

5(a) This section outlines how we will comply with data protection law when processing personal under a lawful basis (see **Appendix 1**), and how we will consider data protection in our business activities.

5.1 Data protection principles

5.1.1 We will process personal data in accordance with the **seven key principles** under the GDPR and DPA 2018:

1. **Lawfulness, fairness and transparency:** We will process personal data under a valid lawful basis (see **Appendix 1** for details on valid lawful bases). We will process personal data in a fair and transparent way, and we will comply with all other applicable law when doing so.

2. **Purpose limitation**: We will have a clear purpose for processing personal data. We will document our purposes and we will only use personal data according to our documented purposes.

3. **Data minimisation**: We will ensure that the personal data we process is adequate, relevant and limited to what is necessary to fulfil our documented purpose for holding that data.

4. **Accuracy**: We will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading.

5. **Storage limitation**: We will not keep personal data for longer than we need it, according to our documented purposes and lawful bases for processing that data.

6. **Integrity and confidentiality**: We will ensure we have appropriate technical and security measures in place to protect personal data.

7. **Accountability:** We will take responsibility for complying with data protection law. We will put measures and documentation in place to evidence our compliance.

5.2 Information Asset Register

5.2.1 We will use our **Information Asset Register** to document which lawful bases we process personal and special category data under. We will ensure our lawful bases are appropriate and our processing is necessary for undertaking our business activities. See **Appendix 1** for more details lawful bases under the GDPR and DPA 2018.

5.2.2 We will also use our **Information Asset Register** to record where we obtain consent from data subjects to process their personal or special category data.

5.3 Collecting and securing personal data

5.3.1 We will periodically review our methods of collecting and processing personal data to ensure these methods remain appropriate.

5.3.2 We will put appropriate organisational and technical measures in place to ensure we process and protect personal data.

5.3.3 See our **ICT Policy** and **Mobile Device Policy** for full details on how we will keep automated personal data secure.

5.4 CCTV

5.4.1 We operate a number of fixed and mobile closed circuit television (**CCTV**) cameras. We operate CCTV cameras to protect our tenants and other residents of the estates that we manage. We also use CCTV cameras to protect our employees and Non-Executive Board/Committee Members, our agents and contractors, and any person lawfully engaged in the locality.

5.4.2 See our **CCTV Policy** for full details on how we use CCTV.

5.5 Data privacy by design and default

5.5.1 We expect all our employees to consider data protection when making changes to any of our business systems, processes, policies and business activities.

5.5.2 The Policy and Information Governance Support Officer must be informed when we propose significant changes to our systems, processes, policies and business activities. The Policy and Information Governance Support Officer will then consider whether a formal Data Protection Impact Assessment is required (see **Section 10.2**).

6. Data subject rights

6(a) The following sections outline our technical and organisational measures to implement data subject rights requests.

6.1 Receiving a request

6.1.1 All actual or suspected data subject rights requests we receive must be reported to the **Policy and Information Governance Support Officer** and a relevant line manager immediately or as soon as possible.

6.1.2 The **Policy and Information Governance Support Officer** will be responsible for coordinating responses to all data subject rights requests.

6.2 Right to be informed: Privacy Notices

6.2.1 A data subject has the right to be informed about the collection and use of their personal data. This includes informing the data subject about purposes for processing their personal data, retention periods for that personal data, and who it will be shared with.

6.2.2 We will provide this privacy information via the following specific Privacy Notices:

- **Privacy Notice for Staff**
- **Privacy Notice for Tenants**
- **Privacy Notice for Non-Executive Board/Committee Members**
- **Privacy Notice on CCHA website**

6.2.3 We will periodically review our privacy notices and update them when necessary. If we change our privacy notices, we will inform our data subjects.

6.3 Right of access: Subject Access Requests

6.3.1 A data subject has the right to access their personal data, commonly referred to as a Subject Access Request (**SAR**). We will respond to all SARs free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.3.2 Where we have doubts about the identity of the requester, we will confirm the identity of the requester before responding to the request. We will inform the requester **within seven days** of the receiving the request if we need further identification.

6.3.3 We may extend our response time to a SAR by up to two months if the request is complex and/or we have received a number of requests from the requester. We will only extend response times when reasonably necessary.

We will inform the requester of the extension within the original one month response time.

6.3.4 In most cases, we will not charge a fee to comply with a subject access request. We reserve the right to charge a reasonable fee for the administrative costs of complying with a request if:

- the request is manifestly unfounded or excessive, or;
- the requester asks for further copies of their personal data following an initial request.

We will inform the requester **within seven days** if we wish to charge a reasonable fee.

6.3.5 When we receive a SAR, we will initially ask the requester to complete a **Data Access Request Form**. We will do this to clarify what personal data is required and to help us locate the personal data. We recognise that the form is not a legal requirement under data protection law. We will comply with a request regardless of whether the form has been completed and returned.

6.3.6 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right of access.

6.4 Right to rectification

6.4.1 A data subject has the right to have their inaccurate personal data rectified, or completed if it is incomplete. We will respond to all requests free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.4.2 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right of rectification.

6.5 Right to erasure

6.5.1 A data subject has the right to have their personal data erased, also known as 'the right to be forgotten'. We will respond to all requests free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.5.2 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right of erasure.

6.6 Right to restrict processing

6.6.1 A data subject has the right to request the restriction or suppression of their personal data. We will respond to all requests free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.6.2 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right to restrict processing.

6.7 Right to data portability

6.7.1 A data subject has the right to obtain and reuse their personal data for their own purposes across different services. This involves moving, copying or transferring personal data easily from one IT environment to another without affecting its usability. We will respond to all requests free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.7.2 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right to data portability.

6.8 Right to object

6.8.1 A data subject has the right to object to the processing of their personal data. We will respond to all requests free of charge and **within one month**, except in certain circumstances and under certain exemptions outlined in data protection law.

6.8.2 See our **Data Subject Rights Procedures** for further details on how we will uphold a data subject's right to object.

6.9 Right related to automated decision-making

6.9.1 We do not undertake any solely automated decision-making. We will monitor our business activities from time to time to ensure this remains true.

7. Data breach management

7(a) This section outlines a definition of a data breach, key responsibilities in managing data breaches under data protection law, and how we will manage data breaches.

7.1 Defining a data breach

7.1.1 A "**data breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The breach of security will also lead to effects on the confidentiality, integrity or availability of personal data. Breaches can result from both accidental and deliberate causes.

7.1.2 We will put appropriate technical and organisational measures in place to detect, investigate, report and manage data breaches.

7.2 Discovering data breaches

7.2.1 All actual or suspected data breaches must be reported to the **Policy and Information Governance Support Officer** and a relevant line manager immediately or as soon as possible.

7.3 Managing data breaches

7.3.1 We will follow a **four-stage** process to manage an actual or suspected data breach. The **Policy and Information Governance Support Officer**, or senior member of staff where more appropriate, will co-ordinate this process.

1. Conduct an internal investigation

We will conduct an internal investigation following an actual or suspected data breach.

2. Assess the risks associated

We will establish the likelihood and severity of the resulting risk to the affected individual's rights and freedoms.

3. Inform the appropriate people

Once the likelihood and severity of the resulting risk of the breach has been established, we will respond as follows:

- If it's likely that there will be a risk to the data subject, we will notify the ICO **within 72 hours**.
- If it is likely that there will be a high risk to the data subject, we will notify the ICO **within 72 hours**, and will also notify all the data subjects affected.
- If it's unlikely that there will be a risk, then we will not report the incident to either the ICO or the data subject's involved.

We will act on a case-by-case basis when deciding whether to notify the ICO of a data breach.

4. **Implement any identified improvements or changes identified**
   We will implement any improvements or changes that are identified during the internal investigation and risk assessment.

7.3.2 See **Data Breach Management Procedure** for detailed guidance on how to manage a data breach.

7.3.3 We will log all data breaches, near miss data breaches and data breach investigation decisions on our **Data Breach & Near Miss Log**.

8. Data sharing

8(a) This section outlines how we will comply with data protection law when sharing personal data.

8.1 Sharing data with third parties

8.1.1 We will not share personal data unless we have a lawful basis or applicable exemption to do so (see **Appendix 1** for details on lawful bases).

8.1.2 We will use the most appropriate lawful basis when we share any personal data with third parties.

8.1.3 We will always apply exemptions on a case-by-case basis.

8.1.4 All our employees will be responsible for ensuring that personal data is shared with third parties in compliance with data protection law.

8.1.5 We will limit access to personal data depending on the assigned duties of our employees, Non-Executive Board/Committee members and associated third parties.

8.1.6 We will periodically review the performance of third parties that process personal data on our behalf, to ensure they are complying with data protection law. If we discover that third parties are non-compliant, we may consider suspending or ending any contractual or similar agreements with that party.

8.1.7 We will use our **Information Asset Register** to document our purposes and lawful bases for sharing personal data.

8.1.8 We will use our **privacy notices** to inform our data subjects of any regular or foreseeable 'one-off' data sharing we undertake (see **Section 6.2**).

8.2 Data sharing agreements and protocols

8.2.1 Where we regularly share personal data with third parties, we will put a **Data Sharing Agreement** in place. We will ensure agreements are accepted and signed by both parties. The agreement will outline who the controller, processer and/or joint controller is, and the responsibilities for each of these under data protection law.

8.2.2 We will ensure that all volunteers, involved tenant representatives and community members or similar complete a **Volunteer Confidentiality and Data Protection Agreement** before handling any personal data on behalf of CCHA.

8.2.2 We recognise the importance of **information sharing protocols** when sharing personal data with other statutory bodies to deliver effective services. We will enter into such protocols as and when they are appropriate.

8.2.3 All **Data Sharing Agreements** or **information sharing protocols** must be signed by either the Head of Governance or the Corporate Director – Central Services.

8.3 Sharing data outside of the UK

8.3.1 We will not transfer personal data outside the European Economic Area ("**EEA**") unless:

A. the country the personal data is transferred to is covered by an '**adequacy decision**' (see link in **Section 14** for current EU Commission 'adequacy decisions');
B. there are '**appropriate safeguards**' in place as defined in data protection law, or;
C. an **exception applies** under data protection law.

8.3.2 We will use our **Information Asset Register** and **Software Compliance Log** to demonstrate our compliance with data protection law when sharing personal data outside of the UK.

9. Data retention and deletion

9(a) This section outlines how we will comply with data protection law when retaining personal data.

9.1 Retaining data

9.1.1 We will only keep personal data for as long as we need it to fulfil our purposes for processing that data.

9.1.2 We will periodically review the personal data we process to ensure that it is accurate and up to date. We will ensure any identified inaccuracies are corrected promptly.

9.1.3 We will adopt the National Housing Federation's best practice guidance on 'Document retention and disposal for housing associations' when retaining data (see **Section 14** for a link to the guidance).

9.1.4 Our **Data Retention Procedure** outlines how long we will retain the personal data we process, and when we will dispose of that data when we no longer need it.

9.2 Disposing of data

9.2.1 We will securely dispose of personal data we process once the need to hold that data has passed.

9.2.2 When disposing of objects that store personal data, we will prioritise physically destroying those objects. We will ensure that destroyed objects are unusable and no personal data can be retrieved from them.

9.2.3 Where objects used to store personal data cannot be physically destroyed, we will ensure those objects are appropriately wiped or altered. We will ensure that wiped or altered objects are unusable and no personal data can be retrieved from them.

9.3 Anonymising data

9.3.1 Where appropriate, we may consider anonymising personal data if there is an identified need to keep that data. If we decide to anonymise data, it will ensure that the data is "rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital 26 – GDPR). Personal data that has been appropriately anonymised will no longer be subject to data protection law.

10. Risk and assurance

10(a) This section outlines how we will monitor data protection risks and provide assurance that we comply with data protection law.

10.1 Monitoring data protection risk

10.1.1 We will periodically review our systems, processes, policies and business activities to ensure the we continue to comply with data protection law.

10.1.2 We will periodically review our key data protection risks during our regular operational risks reviews. See our **Risk Strategy** for further details.

10.2 Data Protection Impact Assessments (DPIAs)

10.2.1 We will complete a Data Protection Impact Assessment (**DPIA**) if we undertake processing that is likely to result in a high risk to our data subjects.

10.2.2 Our **Data Protection Impact Assessment Procedure** outlines how we will assess data protection related risks in regards to our systems, processes, policies and business activities.

11. Training

11(a) This section outlines how we will train our employees in order to maintain our compliance with data protection law.

11.1 We will ensure that our employees and Non-Executive Board/Committee Members are appropriately trained and are aware of their data protection responsibilities under data protection law.

11.2 All our new starters will be required to complete an introduction to data protection induction session as part of our induction programme.

11.3 All our employees will be required to complete an online eLearn module on the essentials of data protection law, alongside refresher modules periodically.

11.4 All our employees will be required to read this policy, and will be required to re-read this policy on an annual basis.

12. Raising a complaint

12.1 External persons

12.1 All external persons who wish to make a complaint about a breach of data protection law or our data protection obligations should use our **Complaints Procedure**.

This includes tenants, service users, housing applicants, employment applicants, contractors, suppliers and other third parties.

CCHA's **Complaints Procedure** which can be found on our website here:

http://www.ccha.org.uk/Compliments_and_Complaints/

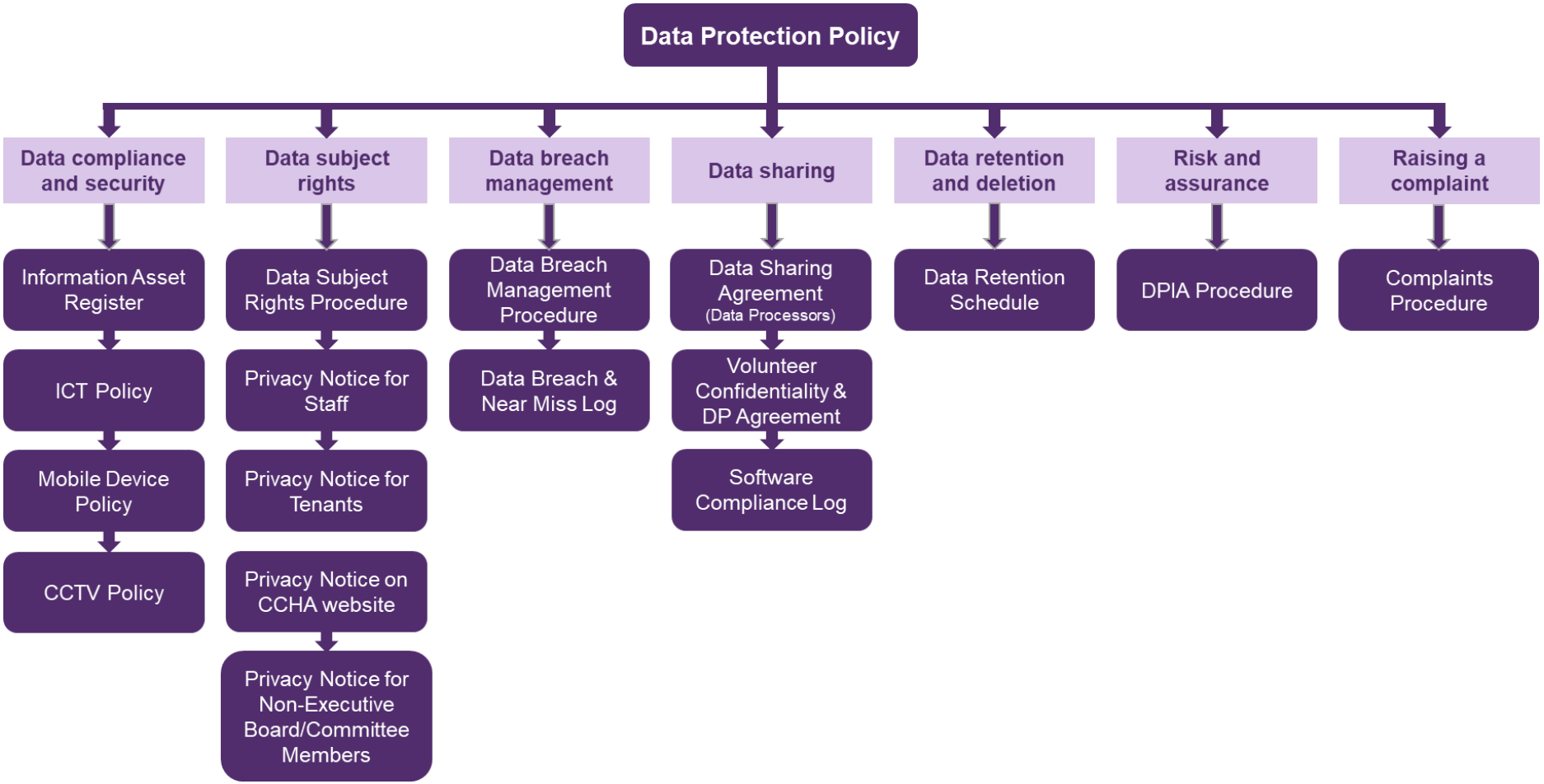
12.2 CCHA employees and Non-Executive Board/Committee Members

12.2 Our employees and Non-Executive Board/Committee Members who wish to make a complaint about a breach of data protection law or our data protection obligations should email the **Data Protection mailbox**:

dataprotection@ccha.org.uk

13. Overview of data protection documents

13(a) This section collates and lists all the data protection-related documentation references in each section above.



14. References

Related External Documents	
Reference	
National Housing Federation's 'Document retention and disposal for housing associations'	https://www.housing.org.uk/resources/document-retention-and-disposal-for-housing-associations/
EU Commission Adequacy Decisions:	https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
Related Internal Documents	
See Section 13.	

15. Document control

Document Information	
Business Owner:	Policy and Information Governance Support Officer – Rhys Jenkins
Version no:	2.0
Effective date:	28th April 2020
Review date:	28th April 2023
Uncontrolled version if printed or emailed. If you are viewing this document from your personal drive, via email or as a hard copy, it may not be the latest version. The current version can be found on the Intranet.	

Document History			
Date	**Version no.**	**Author**	**Description**
May 2018	1.0	GDPR Compliance Officer – Taiwo Idowu	Policy drafted and approved.
April 2020	2.0	Policy and Information Governance Support Officer – Rhys Jenkins	Major review. • Policy re-written. • Reviewed by Head of IT & Procurement and Governance Team. Approved at Audit & Risk Committee on 26/02/2020 and Board decision between meetings on 28/04/2020..

Appendix 1: Guidance on lawful basis for processing

Under data protection law, we must have a valid lawful basis to process personal data. We must also identify a separate legal basis for processing special category data.

A) Lawful bases for processing personal data

There are **six lawful bases** for processing **personal data** as follows:

#	Lawful bases	Description
1	**Consent**	The data subject has given clear consent for us to process their personal data for a specific purpose.
2	**Contract**	The processing is necessary for a contract we have with the data subject, or because they have asked us to take specific steps before entering into a contract.
3	**Legal obligation**	The processing is necessary for us to comply with the law (not including contractual obligations).
4	**Vital interest**	The processing is necessary for us to protect the data subject's life.
5	**Public task**	The processing is necessary for us to perform a task in the public interest, and the task or function has a clear basis in law.
6	**Legitimate interest**	The processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the data subject's personal data which overrides those legitimate interests. This basis is most appropriate where we use personal data in ways a data subject would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Information taken from www.ico.org.uk .		

B) Lawful bases for processing special category data

Under data protection law, we must have a valid lawful basis to process special category data. This lawful basis must be separate from the lawful basis for processing personal data.

There are **ten lawful bases** for processing **special category data** as follows (please note that not all lawful bases are lawfully available and applicable to us):

#	Lawful bases	Description
1	**Consent**	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
2	**Employment, social security and social protection**	The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
3	**Vital interest**	The processing is necessary to protect the data subject's life where the data subject is physically or legally incapable of giving consent.
4	**Legitimate interests**	The processing is carried out in the course of an organisation's legitimate activities (with appropriate safeguards) by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in

#	Lawful bases	Description
		connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
5	**Public data**	The processing relates to personal data which are manifestly made public by the data subject.
6	**Legal obligation**	The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7	**Public task**	The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
8	**Health and medical reasons**	The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the data subject, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to conditions and safeguards.
9	**Public task (public health)**	The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
10	**Archiving**	The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Information taken from www.ico.org.uk.		

C) Processing under consent

Where we process personal and special category data under consent, we will:

- ensure the request for consent is prominent and separate from any other terms and conditions;
- never use pre-ticked boxes or any other type of default consent to obtain consent;
- use clear, plain language when asking a data subject for their consent;
- specify why the data is required and how it will be processed;
- ensure consent is obtained for different purposes of processing, and never use consent from one purpose of processing to cover a different purpose of processing;
- ensure data subjects are aware that they can withdraw their consent;
- avoid making consent a precondition of a service;
- keep a record of consent that has been obtained; and
- periodically review obtained consent to ensure the lawful basis is still relevant.

D) Lawful bases for processing against data subject rights

Under data protection law, not all data subject rights are universally and consistently available to the data subject. The data subject's rights differ depending on the lawful basis selected by the controller of the personal data.

The table below outlines which rights are available to the data subject depending on what lawful basis the personal data is processed under:

		Data subject rights							
		Informed	**Access**	**Rectification**	**Erasure**	**Restriction**	**Portability**	**Objection**	**Automated decision making**
Lawful basis for processing	**Consent**	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
	Contract	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
	Legal obligation	Yes	Yes	Yes	No	Yes	No	No	Yes
	Vital interests	Yes	Yes	Yes	Yes	Yes	No	No	Yes
	Public interest	Yes	Yes	Yes	No	Yes	No	Yes	Yes
	Legitimate interests	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes