Gravesham Borough Council
Data Protection Policy

Document Control

Organisation	Gravesham Borough Council
Title	Data Protection Policy
Author	Preeti Lalli
Filename	GBC Data Protection Policy v1.2
Owner	Information Governance Manager (IG)
Subject	Data Protection Policy
Protective Marking	Official/Unmarked
Review date	January 2025

Revision History

Revision Date	Revisor	Previous Version	Reason for revision
19/01/19	Gayle Jones	1.0	Establish policy in line with the UK GDPR & DPA 2018
12/05/2021	Gayle Jones	1.1	Scheduled review and update in line with UK exit from the EU.
27/01/2023	Preeti Lalli	1.2	Scheduled review

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer (SIRO)	Sarah Parfitt, Director (Corporate Services)	
Management Team	Stuart Bobby, Chief Executive	

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All council employees who handle personal data and Elected Members	All job titles	Via HR's notification of new/updated policy process
All employees of shared services commissioned by the council who handle personal data of which GBC is the data controller.	All job titles	Upon initiation of new contract and annually when contract is renewed.

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Kent County Council

Contents

Busy reader's summary

- Gravesham Borough Council (GBC) is registered under the data protection act with the Information Commissioner's Office (ICO) under registration reference: Z5253191
- This policy applies to all the personal information held by GBC, its subsidiaries and its contractors.
- To be compliant with the UK GDPR, information is collected lawfully and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the company complies with the Data Protection Principles, which are set out in the UK GDPR
- Special conditions are considered when processing Special Category and criminal data
- Individuals must be told how GBC uses their personal information and who it shares with in privacy notices in accordance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 requirements.
- The impact on individual privacy and confidentiality must be understood.
- Personal data must be protected in transit and at rest.
- Anonymisation or pseudonymisation of personal data should be undertaken where the identity of the person serves no purpose.
- Any breaches of personal data or security incidents must be reported to the DPO (gdpr@medway.gov.uk) within 24 hours of becoming aware of the breach.
- International Transfers of personal data is restricted unless certain conditions apply

1. Introduction

The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR) is the law that protects personal privacy and upholds individuals' (sometimes referred to as 'data subjects') rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and processed in accordance with the UK GDPR and current data protection legislation. It will apply to personal information regardless of the way it is used, recorded or stored and whether it is held in paper files or electronically.

2. Policy objectives

2.1 Gravesham Borough Council (GBC) is the Data Controller and as such will comply with its obligations under the DPA and the UK GDPR. GBC is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that its staff and customers are aware of their rights under the legislation.

2.2 All staff must have a general understanding of the law and in particular, know how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

2.3 The Information Commissioner, as the Regulator can impose fines of up to €20 million for serious breaches of the UK GDPR, therefore, it is imperative that GBC and all staff comply with the legislation.

3. Scope

3.1 'Personal data' is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identitiy of a living individual. This includes any expression of opinion about an individual and intentions towards an individual.

3.2 GBC collects and processes a range of information about different data subjects, including amongst other things; name, address, email address, telephone number, date of birth, some protected characteristics and diversity data, and other information including data produced during our interactions. Full details are provided in our Privacy Notice, available on our website.

3.3 This policy applies to all individuals working at all levels at GBC which includes, partners, Council Members, Directors, senior managers, employees, consultants, contractors, graduates, part-time and fixed term workers, casual and agency staff as well as any officer from Medway Council that is supporting the delivery of services through Service Level Agreements.

4. Roles and responsibilities

4.1 All staff (including employees, agency staff, volunteers, freelance consultants, employees on fixed term contracts, and anyone else who may reasonably be described as staff working with GBC are responsible for complying with this Policy, and for reporting any breach of it or suspected breach, to the Information Governance Manager (Data Protection Officer – gdpr@medway.gov.uk).

4.2 Corporate Management team are responsible for promoting the policy to all members of their team(s), and for ensuring that all relevant processes for which they are responsible are designed and carried out in line with this Policy.

4.3 Contractors who are 'Data Processors' are required to comply with this Policy under their contractual obligation. Data Processors have direct responsibilities under the GDPR, including to process personal data only on GBC instructions, to keep it secure, and to cooperate with us as required

4.4 The Data Protection Officer is responsible for advising Gravesham Borough Council about its data protection legal obligations, monitoring compliance, and helping to manage data security breaches and requests from data subjects regarding their data rights.

4.5 The Director (Corporate Services), is the Senior Information Risk Owner (SIRO) and the Assistant Director (IT & Transformation) is the Deputy SIRO.

4.6 The Information Governance Team facilitates GBC's compliance with Information Governance legislation.

4.7 The Information Asset Owner is responsible for maintenance of Records of Processing Activity.

5. Policy Statement

Gravesham Borough Council shall:

- Only use personal data where it is necessary to enable the council to carry out our duties and services.
- Inform individuals how we use their personal data.
- Register itself as a Data Controller with the ICO annually.
- Issue guidance to its staff on compliance with the Data Protection laws.

6. The Principles

The principles set out in the UK GDPR must be adhered to when processing personal information (referred to in the UK GDPR as 'personal data'):

1. Personal data must be processed lawfully, fairly and in a transparent manner ('**lawfulness, fairness and transparency'**).
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**').

   Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed ('**data minimisation**').

   Staff may only process personal information when their role requires it. Staff must not process personal information for any reason unrelated to their role.
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay ('**accuracy**').

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data is processed ('**storage limitation'**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal data are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data ('**integrity and confidentiality'**)

7. Lawful basis for processing personal information

Before any processing activity starts for the first time, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in GBC
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which GBC is subject
- processing is necessary in order to protect the vital interests of the data subject or of another natural person
- processing is necessary for the purposes of the legitimate interests pursued by GBC or by a third party
- the data subject has given consent to the processing of his or her personal information for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal information is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

Staff must be satisfied that the processing is necessary for the purpose of the relevant lawful basis (and that there is no other reasonable way to achieve that purpose)

The decision as to which lawful bases or basis applies must be documented, to demonstrate compliance with the data protection principles. Information must be provided about both the purpose(s) of the processing and the lawful basis for it in GBC's relevant privacy notice(s).

8. Special Categories of Personal Data

Processing of sensitive personal information (known as 'special categories of personal data' in the UK GDPR) is prohibited unless a lawful special condition for processing is identified.

Special category personal data is information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, concerns health, a person's sex life or sexual orientation or is genetic or biometric data which uniquely identifes a natural person.

8.1 **Special category personal information will only be processed if**:

- there is a lawful basis for doing so as identified (see 7 above) and;
- one of the special conditions for processing special category personal information applies:

(a) the individual has given explicit consent

(b) the processing is necessary for the purposes of exercising GBC's or an individual's employment, social security or social protection law rights or obligations

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent

(d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union in relation to its members

(e) the processing relates to personal data which are manifestly made public by the data subject

(f) the processing is necessary for the establishment, exercise or

defence of legal claims or where courts are acting in their judicial capacity

(g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of of social care and the management of social care systems or services

(i) the processing is necessary for reasons of public interest in the area of public health

(j) the processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes (subject to appropriate safeguards).

In addition, Schedule 1 of the Data Protection Act 2018 sets out further conditions and safeguards which must **additionally** be observed when processing special category data:

The additional conditions are that the processing is necessary for:

1. performing obligations or exercising rights in connection with employment, social security or social protection law
2. health or social care purposes (only under obligation of secrecy)
3. archiving purposes, scientific or historical research purposes or statistical purposes in the public interest
4. Specific reasons of 'Substantial Public Interest'

8.2 **Substantial Public Interest**

Purposes for which we process special categories of personal data or criminal information where it is necessary for the substantial public interest include:

- Statutory and government purposes
- Equality of opportunity or treatment (regarding different: race or ethnic origins; religious or similar beliefs; health status; sexual orientation)
- Promoting or maintaining racial or ethnic diversity at senior management levels
- Preventing or detecting unlawful acts
- Protecting the public against dishonesty, malpractice, incompetence and similar
- Preventing fraud
- Making disclosures about suspicions of terrorist financing or money laundering
- Providing confidential advice, support or another similar service provided confidentially
- Safeguarding of children and of adults at risk, including safeguarding of economic well-being
- Insurance purposes
- Occupational pensions
- Responding to requests made by Elected Representatives on behalf of individuals

Personal data will be processed for these reasons only when it is clearly necessary, and in accordance with the other requirements of this Data Protection Policy

8.3 **Criminal Records Information**

Where criminal offence information relating to convictions, offences or related security measures (including personal information relating to the alleged commission of offences by an individual or proceedings for an offence committed or alleged to have been committed, including sentencing) is processed, a lawful condition for processing that information must also be identified and documented as set out in Schedule 1 of the Data Protection Act 2018. These include:

- consent
- protecting a person's vital interests
- personal data in the public domain
- legal claims
- judicial acts
- any of the conditions listed under substantial public interest
- insurance.

A policy document must also be in place and retained, and a record of processing kept as for special category personal information.

Where GBC is relying on certain additional conditions in the DPA as outlined above at 8.1 (employment etc obligations) or 8.2 (substantial public interest) or as set out in section 8.3 (criminal convictions) the following safeguards must also be in place:

- an appropriate policy document which explains the procedure for complying with the UK GDPR Principles (set out in section 6 above) when relying on these additional conditions

- an appropriate policy document that explains the retention and erasure of information processed under the additional conditions. (See GBC's Retention Schedule in relation to this)
- the policy document(s) must be retained for at least 6 months after processing has ended, regularly reviewed and updated and available to the ICO upon request
- a record must be maintained of the processing of personal data in reliance on these conditions which specifies:
    a) the condition relied on
    b) how it satisfies Article 6 (lawful bases of processing) and
    c) whether personal data is retained and erased in accordance with GBC's Retention Schedule and if not, the reasons why.

GBC's privacy notice(s) set out the types of special category personal information that it processes, what it is used for, the lawful basis for the processing and any exceptions or conditions that are relied upon.

Special category personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where explicit consent is required for processing special category personal information, evidence of consent will need to be captured and recorded so that GBC can demonstrate its compliance with the law.

9. Automated Decision Making

Where GBC carries out automated decision making (including profiling) it must meet all the principles set out in section 6 above and have a lawful basis for the processing cited in a privacy notice. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. GBC must as soon as reasonably possible notify individuals in writing that a decision has been taken based on solely automated processing and that they may, within 1 month of receiving the notification, request reconsideration or a new decision. If such a request is received staff must contact the DPO and GBC must reply within 1 month, in certain circumstances the GDPR allows an extension of 2 further months.

10. Data Protection Impact Assessments

10.1 Gravesham Borough Council's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles (such as data minimisation).

10.2 Where processing is likely to result in high risk to an individual's rights and freedoms (for example where a new technology is being implemented or if it will involve largescale processing of sensitive personal information or information relating to criminal offences) a Data Protection Impact Assessment (DPIA) must be carried out.

10.3 During the course of any DPIA, staff should seek the advice of the Information Governance Manager and keep it under review throughout the lifetime of the project concerned.

11. Records of Processing Activities

Gravesham Borough Council must maintain a written record of processing activities (also known as ROPA) which should include:

- the name and details of the Directorate and service carrying out the processing
- the purposes of the processing
- the lawful basis for the processing
- a description of the categories of individuals and categories of personal data
- whether personal information of children is being processed
- details of the recipients of personal information
- where relevant, details of transfers to countries outside of the EEA or to international organisations, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures in place.

All Information Asset Owners for GDPR should conduct regular reviews of the personal information GBC processes within their service and update ROPA accordingly.

12. Privacy notices

12.1 GBC will issue privacy notices from time to time as required, informing individuals about the personal information that it collects and holds and details of how individuals can expect their personal information to be used and for what purposes.

12.2 When information is collected directly from individuals, including for HR or employment purposes, the individual shall be given all the information required by the UK GDPR including the identity of the data controller and the DPO, how and why GBC will use, process, disclose, protect and retain that personal information through a privacy notice (which must be presented when the data subject first provides the personal information).

12.3 When information is collected indirectly (for example from a third party or publically available source) the individual must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the personal information and no later than one month from that date. We will also inform the data subject about:

- The categories of personal data concerned
- The source of personal data

12.4 GBC will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

13. Individual rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed (see GBC's privacy statement and privacy notice(s))
- confirmation that personal information is being processed and to **obtain access** to it and certain other information, via a subject access request
- to have personal information **corrected** if it is inaccurate or incomplete
- to have personal information **erased** if it is no longer necessary for the purpose for which it was originally collected/processed or when the consent on which the processing is based has been withdrawn and there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- to **restrict** the processing of personal information where the accuracy of the information is contested, or the processing is unlawful or where the personal information is no longer needed by GBC but the individual requires it to establish, exercise or defend a legal claim, and
- to **restrict** the processing of personal information temporarily where an individual does not think it is accurate (and GBC is verifying whether it is accurate), or where an individual has objected to the processing (and GBC is considering whether its legitimate grounds override an indivudal's interests)
- in limited circumstances to receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine readable format
- where processing of personal information is based on consent, to withdraw that consent at any time
- to request a copy of an agreement under which personal information is transferred outside of the EEA
- to object to decisions based solely on automated processing, including profiling
- to make a complaint to the ICO or a Court.

Anyone wishing to exercise any of the rights above, or who receives a request from someone else to exercise any of the rights above, should contact gdpr@medway.gov.uk.

Gravesham Borough Council aims to fulfil all valid requests within one month unless there is a good reason to lawfully extend the timescale by up to an extra 2 months.

14. Individual responsibilities

Individuals are responsible for helping GBC keep their personal information up to date. Staff can update their own information via the employee self service portal.

Staff may have access to the personal information of other members of staff, suppliers, clients or the public in the course of their employment or engagement. If so, GBC expects staff to help meets its data protection obligations to those individuals. For example, staff should be aware that those individuals may enjoy the rights set out above.

If staff have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes
- only allow other GBC staff to access personal information if they have appropriate authorisation
- only allow individuals who are not GBC staff to access personal information if they have specific authority to do so
- keep personal information secure (e.g. by complying with council policies and guidelines, with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with GBC's policies, associated policies as per policy list below)
- not remove personal information, or devices containing personal information (or which can be used to access it) from the council's premesis unless appropriate security measures are in place (such as pseudonymisation or encryption) to secure the information and the device; and comply with GBC's Removeable Media Policy, Information Protection Policy and Hybrid Working Policy.
- not store personal information on local drives or on personal devices that are used for work purposes and comply with the council's Remote Working Policy.

15. Information security

GBC will use appropriate technical and organisational measures in accordance with its Information Security Policy to keep personal information secure, and in particular, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Staff are responsible for keeping information secure in accordance with the Information Security Policy and must read that policy in conjunction with this one.

Staff must follow all procedures and technologies put in place to maintain the security of all personal information from the point of collection to the point of destruction. Staff may only transfer personal information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity, resilience and availability of the personal information, defined as follows:

(a) confidentiality means that only people who have a need to know and are authorised to use the personal information can access it

(b) integrity means that personal information is accurate and suitable for the purpose for which it is processed

(c) availability means that authorised users are able to access the personal information when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards GBC has implemented and maintains in accordance with the UK GDPR.

Where GBC uses external organisations to process personal information on its behalf, additional security arrangements must be implemented in contracts with those organisations to safeguard the security of personal information.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms from Legal Services.

16. Storage and retention of personal information

16.1 Personal information will be kept securely in accordance with GBC's information security policies and data protection obligations.

16.2 Personal information must not be retained for any longer than necessary. The length of time personal information should be retained will depend upon the circumstances, including the reasons why personal information was obtained. Staff should adhere to GBC's Records Management Policy with reference to its Retention Schedule.

16.3 Personal information that is no longer required will be deleted permanently from GBC's information systems and any hard copies will be destroyed securely.

17. Data breaches

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored
- unauthorised access to or use of personal information either by a member of staff or third party
- loss of data resulting from an equipment or systems (including hardware or software) failure
- human error, such as accidental deletion or alteration of data or emailing the wrong individual or pressing 'reply all' instead of 'reply'
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- blagging offences where information is obtained by deceiving the organisation which holds it

If GBC becomes aware of a data breach that is likely to result in a risk to individuals' rights, it must report it to the Information Governance Team or directly to the DPO via gdpr@medway.gov.uk

Staff must inform their service manager immediately if a data breach is discovered and make all reasonable efforts to recover any information. Staff and managers must have regard to GBC's Data Breach Policy.

18. Training

Gravesham Borough Council will ensure that staff are adequately trained regarding their data protection responsibilities. All staff are required to complete mandatory information governance and data protection training every two years.

19. Consequences of a failure to comply

19.1 Gravesham Borough Council takes compliance with this policy very seriously. Failure to comply puts data subjects at risk and carries the risk of significant civil and criminal sanctions for the individuals responsible and for GBC and may in some circumstances amount to a criminal offence by the individual.

19.2 Any failure to comply with any part of this policy may lead to disciplinary action under GBC's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If staff have any questions or concerns about this policy they should contact their line manager or the Data Protection Officer.

20. Review of policy

This policy will be reviewed by the Information Governance Manager, IGSG every 2 years. In addition, changes to legislation, codes of practice or commissioner's advise may trigger interim reviews.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: means 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. It is responsible for establishing practices and policies in line with the UK GDPR. Gravesham Borough Council is the Data Controller of all personal information relating to its clients, customers and staff.

Data Subject: a living, identified or identifiable individual about whom GBC holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of **Privacy by Design** and should be conducted for all major systems or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the UK GDPR.

EEA: the 27 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK General Data Protection Regulation (UK GDPR): the UK General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: is any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identitiy of that natural person.

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.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR such that necessary safeguards are integrated into the processing from the outset.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when GBC collects information about them. These notices may take the form of general **privacy** statements applicable to a specific group of individuals (for example, employee **privacy** notices or the website **privacy** policy) or they may be stand-alone, one time **privacy** statements covering Processing related to a specific purpose.

Processing: means anything done with 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: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation: means processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.