Criminal Conviction and Special Category Data Policy

1.0 Policy Statement

This policy sets out Gloucestershire County Council's (the council) processing of special categories of personal data (special category data) and personal data relating to criminal convictions and offences (henceforth criminal conviction data). It is intended to guide council staff in what to consider when processing these types of data and how to meet the requirements set out in Data Protection Legislation.

This policy also serves as the Appropriate Policy Document for special category and criminal conviction data as required by Schedule 1, Part 4 of the Data Protection Act (DPA) 2018. The policy document explains;

- the council's procedures for ensuring compliance with the principles in Article 5 of the UK General Data Protection Regulation (UK GDPR) when processing of special category or criminal conviction data, and,
- where the council's policies on the retention and erasure of special category data, criminal conviction data and Record of Processing Activities (ROPA) can be found.

All members and officers of the council should be aware of this policy and in particular the safeguards set out in Section 7.0. Service Leads and Information Asset Owners (IAOs) should engage with the Information Management Service (IMS) where their services process special category data or criminal conviction data.

2.0 What is Special Category Data

Article 9 of the UK GDPR sets out that special category data consists of personal data that includes:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade Union membership,
- Genetic data,
- Biometric data for the purpose of identifying an individual,
- Health or data about an individual's physical or mental condition,
- Data concerning a person's sex life or sexual orientation.

Special category data does not include personal data relating to criminal convictions and offences, this information is treated differently under data protection legislation.

2.1 Identifying Inferred Special Category Data

There are some types of processing data that does not directly collect Special Category data as identified above, however, due to the nature of the processing an individual's special category data can be inferred from what has been collected.

For example, a service who is providing a service for those with disabilities. Whilst they may not be directly collecting data about the service users' medical conditions it may be possible to infer information about the persons health conditions from the fact that they are accessing the service.

In cases such as this, council officers should seek advice from the Information Management Service.

3.0 What is Criminal Conviction Data

Chapter 2, Part 2, Section 11 of the DPA 2018 states that criminal conviction data constitutes:

> "Personal data relating to criminal convictions and offences or related security measures include personal data relating to:
> (2)(a) The alleged commission of offences by the data subject, or;
> (2)(b) Proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing."

The council has interpreted the definition of (2)(a) as being met where:

- the council intends to report the individual to a relevant authority due to an allegation,
- where the police or another authority have advised us of alleged criminal offences and convictions, or
- where the council has legal powers to carry out an investigation itself.

Criminal conviction data may exist as a record in its own right, or it may form part of a larger record that contains other types of personal or special category data, such as a social care or safeguarding record.

3.1 Criminal Conviction Data processed by suppliers

There is an important exemption when the council commissions a service that regularly and intentionally processes data about prior criminal convictions, allegations, or police involvement. In these cases, if the data is provided by:

- the data subject themselves, or
- social Services,

then it is still classified as criminal conviction data, even if the council is not directly involved in the processing of such data.

4.0 What the legislation says

4.1 Special Category Data

Article 9(1) of the UK GDPR states that processing of special category data is prohibited, unless a specific condition from Article 9(2) can be met.

These conditions are:

- 9(2)(a) The data subject has given explicit consent to the processing,
- 9(2)(b) Processing is necessary in the field of employment and social security and social protection law
- 9(2)(c) Processing is necessary in order to protect vital interests of the data subject or another data subject
- 9(2)(d) Processing is necessary for the legitimate activities of a not-for-profit body
- 9(2)(e) Processing relates to personal data which are manifestly made public by the data subject
- 9(2)(f) Processing is necessary for legal claims
- 9(2)(g) Processing is necessary for reasons of substantial public interest
- 9(2)(h) Processing is necessary for the provision and/or management of health and/or social care systems
- 9(2)(i) Processing is necessary for reasons of public interest in the area of public health
- 9(2)(j) Processing is necessary for archiving purposes in the public interest

In addition to this, Sections 10(1-3) of the DPA 2018 makes it clear that where conditions

- 9(2)(b) (employment, social security and social protection),
- 9(2)(h) (health and social care),
- 9(2)(i) (public health), and
- 9(2)(j) (archiving, research and statistics),

are relied upon then **a condition from Part 2 of Schedule 1 of DPA 2018** must also be met. These conditions are:

1. Employment, Social Security, and Social Protection

You can process sensitive personal data if:

- it's required by law to carry out your duties or rights related to employment, social security, or social protection (like pensions or welfare benefits).
- you have a policy document in place that explains how you handle and protect this data.

2. Health or Social Care Purposes

You can process sensitive data if it's necessary for:

- Preventive or occupational medicine (e.g. health checks at work),
- Assessing an employee's ability to work,

- Medical diagnosis,
- Providing health care or treatment,
- Providing social care, or
- Managing health or social care systems.

This must also comply with confidentiality rules under UK GDPR and other laws.

3. Public Health

You can process sensitive data if:

- it's needed for public interest reasons in the area of public health (like controlling disease outbreaks), and
- it's done by a health professional or someone who is legally required to keep the information confidential.

If condition

- 9(2)(g) (substantial public interest)

is relied upon then **a condition from Part 2 of Schedule 1 of DPA 2018** must also be met.

4.2 Criminal Conviction Data

In order to comply with the GDPR when processing criminal conviction data, the council must have a lawful basis under Article 6(1) and either legal or official authority for the processing under Article 10.

Article 10 states:

> "Processing of personal data relating to criminal convictions and offences or security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

This means that the council must either:

- process the data in an official capacity; or
- meet a specific condition in Schedule 1 of the DPA 2018, and comply with the additional safeguards (Schedule 1, Part 4) set out in that Act.

Note: Even if the council has a condition for processing offence data, the council can only keep a comprehensive register of criminal convictions if it does so in an Official Capacity.

The Law Enforcement Directive (LED), enacted in the UK as Part 3 of the DPA 2018, sets out rules for how **competent authorities** (e.g. police, prosecutors, and other

public bodies with law enforcement powers) must handle **personal data** when it's processed for **criminal law enforcement purposes**.

These purposes include:

- Prevention
- Investigation
- Detection
- Prosecution of criminal offences
- Execution of criminal penalties
- Safeguarding against and prevention of threats to public security

4.3 What the legislation says about the use of AI with Criminal Convictions Data

The Data Use and Access Act 2025 has set out guidelines on how the Council may use automated processing for significant decision making in relation to personal data. Automated decision making is when a decision is made without meaningful human involvement in the making of said decision.

A decision is considered ‘significant’ if, in relation to a data subject, it produces a legal effect for the data subject or if it produces a significant effect for the data subject.

For example, the Council receives a referral about a child potentially at risk. An automated system processes personal data, including school attendance, previous social care involvement, and police reports, and generates a risk score suggesting the child may be at high risk. The system’s score automatically triggers a decision to escalate the case to a child protection investigation. No social worker reviews the data or questions the outcome, and the family is contacted based solely on the automated result.

A legal effect means the decision changes the legal rights or obligations of the child or their family. In this case, examples include triggering a statutory child protection investigation or placement of the child on a Child Protection Plan.

A significant effect refers to the substantial impacts on an individual's life, in this case it could be emotional distress, stigma or reputational harm, impact on the child’s wellbeing, disruption to family life or a loss of trust in social care services. These effects may not change the legal rights, but they materially affect the child’s and families' circumstances, choices and relationships. The above scenario is without meaningful human involvement. To contain meaningful human involvement the process may look like a qualified social worker reviewing the automated risk score alongside the underlying data. They consider contextual factors not captured by the system (e.g. recent family support, school feedback, or cultural considerations). The

social worker makes the final decision, documenting their reasoning and explaining how the automated analysis informed but did not dictate the outcome. The family is informed of the decision and given an opportunity to respond or provide further information.

A ‘significant decision’ may not be taken based solely on automated processing if the processing of personal data carried out by, or on behalf of, relies entirely or partly on Article 6(1)(e).

Article 6(1) (e) refers to the lawful basis for processing personal data for tasks carried out in the public interest, particularly those related to safeguarding children and individuals at risk.

The Council is allowed to use automated processing if one the following conditions are met:

1. *The decision is based entirely on the processing of personal data which the data subject has given explicit consent*
2. *The decision is necessary for entering into or performing a contact between the data subject and the controller or is required or authorised by law.*

Importantly, you cannot rely on ‘legitimate interests’ as a legal basis for fully automated decision-making involving this type of data.

Note: ‘Recognised legitimate interests’ refer to specific statutory interests (e.g. crime prevention). However, these cannot be used alone to justify automated decision-making without meaningful human involvement.

Where a significant decision has been made by, or on the behalf of, the Council in relation to a data subject, based entirely or partially on personal data **and** based solely on automated processing, the Council must ensure that there are safeguards in place to protect the rights and freedoms of the data subject. These safeguards must consist of and include the following measure, as per section 50C of the Data (Use and Access) Act 2025:

1. Provide the data subject with information about the automated decision making in relation to their information
2. Enable the data subject to make representations about automated decisions
3. Enable the data subject to have human intervention on the part of the council in relation to automated decision making
4. Enable the data subject to consent to automated decision making.

Example:

A council's AI system cannot fully automate a decision about an individual's eligibility for a service based on health or criminal data unless the person has explicitly consented or the decision is authorised by law under strict conditions.

5.0 Processing of Criminal Conviction Data in an Official Capacity or as a Competent Authority

As per Section 8 of the DPA 2018, the council is deemed to be working in an Official Capacity or Official Authority when processing personal data that is necessary for the exercise of a function conferred on it by an enactment or activity. Official Authority can also include council powers that are not necessarily set out in legislation, such as our powers as a Highway Authority, the Fire and Rescue Authority or the Trading Standards Authority.

Under the Law Enforcement Directive (LED), the council is considered a Competent Authority when processing personal data is necessary for its law enforcement-related functions, such as Trading Standards or Internal Audit. The council also qualifies as a Competent Authority when processing is required to fulfil its responsibilities under the Prevent Duty. However, if a Competent Authority processes personal data for purposes other than law enforcement, that processing falls under the general data protection regime outlined in Part 2 of the Data Protection Act 2018. Being a Competent Authority does not create a general power to disclose, receive or reuse personal data. The Council must identify the specific statutory function, legal gateway or legislative power that permits the processing in each case. Information obtained under a Memorandum of Understanding or other sharing arrangement may be subject to additional restrictions on reuse or onward disclosure

The table below details which legislation applies to each type of processing:

Processing Activity	**Legislation**
Where the council is acting as a competent authority	Part 3 and Schedule 8, DPA 2018 (LED)
Where the council is not acting as a competent authority, but the information relates to a criminal offence	Parts 1, 2, and 3 of Schedule 1, DPA 2018
Where the information relates to civil offences	GDPR

6.0 Meeting a Schedule 1 condition

Where an organisation doesn't have Official Capacity, it must meet a specific condition in Schedule 1 of the DPA 2018. Parts 1 to 3 of that schedule provide a number of conditions to meet the requirements set out by section 10. Below are examples of where the council processes criminal conviction data and the Schedule 1 conditions that are most appropriate for that processing.

Note: These conditions only cover the lawfulness aspect of the first principle. Any processing of personal data using one of these conditions should still consider the fairness, transparency and adequacy of the processing.

Example:	**Schedule 1, Part 1, 2 or 3 condition(s):**	**Type of Applicable data**
Recruitment; undertaking pre-employment checks; HR investigations; change in personal circumstances, processing information relating to Trade Union Membership and strike action, including deducting Trade Union membership from payroll	**Part 1(1)(1)(a)** – with obligations in connection with employment, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment	**Special category and Criminal Convictions data**
Adult and Children Social care and/or Safeguarding	**Part 1(1)(1)(a)** – with obligations in connection with social security or social protection, or; **Part 1(2)(1)** – necessary for health or social care purposes, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment; or **Part 2(18)(a)** – necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm.	**Special Category Data and Criminal Convictions data**
Multi-Agency Risk Assessment Conference (MARAC) – Gloucestershire Domestic Abuse project	**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment	**Criminal Convictions data**
Youth Offending Support	**Part 1(2)(1)** – necessary for health or social care purposes, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment, in particular permitted by: Section 115 of the Crime and Disorder Act 1998, and Section 14 of the Offender Management Act 2007.	**Criminal Convictions data and Special Category data**

Example:	Schedule 1, Part 1, 2 or 3 condition(s):	Type of Applicable data
Trading Standards; Licensing; meeting legislative requirements for responding to unlawful acts	**Part 2(12)** – necessary for the purposes of complying with a regulatory requirement which involves establishing whether a person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct; **Part 2(11)** – necessary for the exercise of a protective function in protecting/ the public against dishonesty, malpractice or other seriously improper conduct	**Criminal Convictions Data**
Archiving, statistical or historical research	**Part 1(4)** – necessary for archiving, statistical or historical research purposes that are in the public interest (and in accordance with Article 89)	**Criminal Convictions data and special category data**
Community safety and functions in respect of crime and disorder	**Part 2(10)(a)** – necessary for the purposes of the prevention of detection of an unlawful act, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment (depending on whether the Council has official authority).	**Criminal Convictions data or Special category data**
Preventing fraud or disclosing information to an anti-fraud organisation	**Part 2(14)(a)** – necessary for the purposes of preventing fraud or a particular kind of fraud.	**Criminal Convictions data and Special Category data**
Investigations by the Council's Internal Audit team into allegations of fraud or misspending of public funds	**Part 2(14)(a)** – necessary for the purposes of preventing fraud or a particular kind of fraud. **Part 2(10)(a)** – necessary for the purposes of the prevention of detection of an unlawful act, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment (depending on whether the Council has official authority).	**Criminal Convictions data**

Example:	Schedule 1, Part 1, 2 or 3 condition(s):	Type of Applicable data
Disclosure to elected representatives responding to requests from constituents	**Part 2(24)** – the processing consists of the disclosure of personal data to an elected representative or person acting under their authority.	**Criminal Convictions data or special category data**
Disclosure as part of a Data Subject Access request.	**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment.	**Criminal Convictions data or special category data**
Disclosure as part of a request from the Police or another authority to support with investigations	**Part 2(10)(a)** – necessary for the purposes of the prevention of detection of an unlawful act, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment	**Criminal Convictions data or special category data**
Equalities Monitoring	**Part 2(8)** – necessary for the purposes of equality of opportunity, or**;** **Part 2(9)** – necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment**.**	**Special Category Data**
Public health	**Part 1(2)(1)** – necessary for health or social care purposes, or; **Part 1(3)** – necessary for the reasons of public interest in the area of public health, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment.	**Special Category Data**

7.0 Appropriate Policy Document and Additional Safeguards

Schedule 1, Part 4, of the DPA 2018 requires the council to create and maintain an Appropriate Policy Document and keep a Record of Processing Activities in relation to processing of criminal conviction data.

7.1 Appropriate Policy Document

The following statements explain how the council meets the requirements of the Principles from Article 5 of the GDPR in connection with the processing of special category and criminal conviction data.

Principle 1 – Lawful, fair and transparent

The council will;

- ensure that special category and criminal conviction data is only processed where a lawful basis applies.
- ensure that processing does not take place unless the reason for processing is derived from a lawful basis from Article 9 of the UK GDPR (see Section 3.0) and if necessary, a Schedule 1 condition from DPA 2018 (see Section 4.0) and does not infringe data protection legislation or any other law.
- ensure that processing does not take place unless the reason for processing is derived from legal powers granted to the council and it does not infringe data protection legislation or any other law.
- only process personal data fairly and ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information about the processing, unless an exemption applies.
- complete a Data Protection Impact Assessment (DPIA) for any high risk processing involving the use of criminal conviction data. The assessment should be completed by the relevant Information Asset Owner (IAO).

When sharing data that is DWP derived you will not need to comply with the data re-use process enforcement if you are sharing the data with law enforcement authorities. If you are not sharing for this purpose you will need to complete a DWP Memorandum of Understanding Re-Use Form.

Principle 2 – Purpose limitation

The council will:

- only process personal data for specific and explicit purposes which will be included within the relevant Privacy Notice, unless an exemption applies.
- not use personal data for purposes that are incompatible with the purposes for which it was collected unless required by law. We will inform data subjects of this change unless a relevant exemption applies or required by law not to disclose the new purpose.
- where a council service wishes to use personal data for a different purpose they should consult IMS for advice.

Principle 3 – Data minimisation

The council will ensure that special category and criminal conviction data processed by the council shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4 – Accuracy

The council will:

- ensure that special category and criminal conviction data is accurate and where necessary kept up to date.
- ensure that data quality is maintained in line with the council's Data Quality Standards.
- ensure that a distinction between the data relating to the below categories of data subjects is made;
    - Suspects,
    - Those convicted of criminal offences,
    - Victims, and
    - Witnesses or individuals with information about offences.
- personal data based on a personal assessment and opinion (including intelligence) must be distinguished from that which is based on fact.

Principle 5 – Storage Limitation

All special category and criminal conviction data will be retained in accordance with the council's Records Retention and Disposal Schedule.

Principle 6 – Security

Information processed for a law enforcement purpose and special category data must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The council's Information Security Policy sets out the security requirements internally, and the Cyber and Information Management (Procurement) Policy sets out the security requirements for third party suppliers (processors).

The council has a wide range of technical and procedural controls in place, in order to protect the special category and criminal conviction data it processes. These controls are overseen by the council's Information Board and the Senior Information Risk Owner (SIRO), supported by a network of IAOs.

These controls include, but are not limited to;

- mandatory information security training for all staff.
- mandatory acceptance of Data Protection, Information Security and IT Access policies by all staff.
- encryption of data in transit (i.e. secure email) where appropriate.
- appropriate levels of encryption, firewalls and business continuity arrangements for corporately servers holding personal data. Council hosted systems are located in the UK and accredited to ISO 27001.
- contracts with processors and suppliers that contain appropriate GDPR and data protection clauses.

- controlled access (such as role-based access controls) for systems holding special category and/or criminal conviction data.
- corporately backed data protection by design processes and culture to ensure information security are considered and implemented, via Data Protection Impact Assessment's where appropriate, prior to the processing of personal data.
- ID badges to control access to council buildings, which is reinforced by controls to confirm authenticity of badges by machine and by staff.
- an established Information Security Incident procedure, to mitigate risk and ensure the council complies with its legal obligations where potential breaches may have occurred.

Principle 7 – Accountability

The council must be responsible for and demonstrate compliance with these principles. The council will:

- ensure that records are kept of all processing activities involving special category and criminal conviction data (see section 7.3 below).
- ensure that IAOs will complete a Data Protection Impact Assessment for any high-risk processing involving the use of special category data or criminal conviction data.

The council has appointed a Data Protection Officer whose role is to provide independent advice on data protection to the council, and to monitor compliance with relevant data protection legislation.

7.2 Retention of Appropriate Policy Document

- the policy document will be retained for the length of the processing of special category data and criminal conviction data plus six months
- the council will review the policy on an annual basis, as per Information Commissioner's Office (ICO) guidance.
- the council will make the policy available to the ICO upon request and without charge.

7.3 Record of Processing

The council maintains a Record of Processing Activities via the Information Asset Register (IAR). The information included in the ROPA includes

- which processing condition of Schedule 1, Parts 1 to 3 are relied upon,
- how the processing satisfies Article 6 and 9 of the UK GDPR, and
- the retention periods for data.

IAOs and Information Asset Managers are provided with access to the IAR by the Information Management Service. IAOs are accountable for ensuring that the Information Asset Register is kept accurate and up to date.

7.4 Data Subject Rights

Details of individual's rights and how they access their information can be found in the Information Rights Policy , along with further supporting procedures this can be found on the council's My information rights pages.

8.0 Agents, partners organisations and contractors

If a contractor, partner organisation or agent of the council is appointed or engaged to collect, hold, process or deal with criminal conviction data on behalf of the council, or if they will do so as part of the services they provide to the council, the lead council officer for that service must ensure that appropriate contractual clauses for security and data protection requirements are in place. Personal data must be processed in accordance with the principles of data protection law and this policy.

9.0 Further information

For further information or specific guidance please visit the IMS pages on Staffnet or contact dpo@gloucestershire.gov.uk.

10.0 Related polices

When reading this policy consideration must also be made to the below policies and guidance, which are available on the council's Information Management and Security Policies pages;

- Data Protection Policy
- Information Security Policy
- Information Management Principles
- Internet and Digital Communications Policy
- Information Rights Policy
- Information Sharing
- Information and Records Management Policy
- Records Retention and Disposal Schedule
- Data Quality Standards
- Generative AI Policy

11.0 Document Control

11.1 Document information

Owner:	Nick Holland, Data Protection Officer
Author:	Nick Holland, Data Protection Officer
Reviewer:	Nicole Barrow, Information Governance Adviser
Board(s) consulted:	
Date created:	April 2026
Next review date:	September 2027
Approval:	
Date of approval:	
Scheme of Delegation ref:	
Version:	1.1
Classification:	UNCLASSIFIED

11.2 Version History

Version	Version date	Summary of Changes
1	April 2026	Original Version – Combination of Special Category Data Policy v1.5 and Criminal Conviction Data Policy V1.3
1.1.	September 2026	Updated sections on Processing of Criminal Convictions data and Schedule One to include requirements for the re-use of DWP Data as per the DWP MOU.

11.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

11.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000

12.0 Appendices

12.1 Abbreviations & Glossary

Abbreviation	Description
IMS	Information Management Service
IAO	Information Asset Owner
ICO	Information Commissioner's Office
DPA	Data Protection Act 2018
FoIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
SAR	Subject Access Request

Glossary	Description
Data Controller	The individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Protection Officer (DPO)	The DPO is a statutory role that assists organisations with monitoring internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority.
Data Subject	The individual who the personal data or information is about
Information Asset Owner (IAO)	An Information Asset Owner is a member of staff whose seniority is appropriate for the value of the asset they own. Information owners are business managers who operationally own the information contained in their systems (paper and/or electronic). Their role is to understand what information is held, how it is used and transferred, and who has access to it and why, in order for business to be transacted within an acceptable level of risk.
Information Commissioner's Office (ICO)	The supervisory authority who has responsibility to see that the GDPR and DPA is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the GDPR.
Personal Data	The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier
Processing	Covers a broad range of activities involving personal data, such as collecting, storing, reviewing, editing, deleting, sharing and permanent preservation. It is expected that any use of personal information or data by the Council will amount to processing.

Glossary	Description
Sensitive (Special Category) Data	Information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.
Subject Access Request (SAR)	An individual's request for personal data under the GDPR.
Criminal Convictions Data	Information about personal data relating to criminal convictions and offences or related to security measures. This includes information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It encompasses other personal data that is linked to criminal offences or data that is used to learn about an individual's criminal record or behavior.
Official Capacity	Refers to actions or responsibilities carried out by someone as part of their formal role or job, especially within an organization, government, or legal context.
Official Authority	Official authority refers to the legal or formal power granted to an organization to make decisions, enforce rules, or carry out duties. It's the recognized right to act on behalf of a body, such as a government, council, or company.
Competent Authority	A competent authority is a person or organization that has been legally empowered, usually by statute or regulation, to carry out specific functions within a defined area of responsibility.
Automated Decision Making	Decisions made **solely by automated means** without any human involvement, which have **legal effects** or **similarly significant impacts** on individuals