Policy Number	66
Level	3
Issue	3
Issue date	01/08/2018
EIA	01/08/2018
Review Date	01/05/2021
Author	Nick Murton
SMG approval	28/6/2018

Edinburgh College

For the future you want

Data Protection Policy

Corporate Development

Contents

1. INTRODUCTION

This is the Edinburgh College Data Protection Policy. It sets out the legal framework and risks which govern our use of data; the college's commitment to protecting its data; and the obligations of users to protect all data (with particular reference to personal and special (previously called sensitive) categories of personal data).

It applies to all managers, employees, contractors and anyone else who can access or use data in their work for the college.

It should be read in conjunction with the college's Information Security and IT Facilities Acceptable Use policies.

Any concerns about the protection of data at Edinburgh College, or non-compliance with this policy, must be reported to DP@Edinburghcollege.ac.uk immediately.

2. PURPOSE

In undertaking the business of Edinburgh College we create, gather, store and process large amounts of data: this includes personal and special categories of personal data, which are subject to data protection laws.

Edinburgh College is committed to a policy of protecting data, and to protecting the rights and freedoms of individuals with respect to the processing of their personal data. Protecting data, and particularly individuals' personal data, is consistent with college values ("trustworthy"). It is also consistent with the right to privacy expressed in both the European Convention on Human Rights (ECHR) (Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society") and the UN Convention on the Rights of the Child (UNCRC) (Article 16: Every child has the right to privacy). It also supports a number of the College's strategic aims: valued in partnership and by communities ("EC is a trusted partner"); effective and efficient college ("strong

corporate controls; high standards of governance; assured Board of Management, staff, students, funders and partners").

This policy, and associated procedures, support the college's compliance with its obligations as a Data Controller and where applicable, a Data Processor, under data protection legislation.

The effective management and control of data enables the college to effectively secure data; retrieve data when required; trust its currency and accuracy, and use it to support effective and efficient decision making.

This policy sets out data users' roles and obligations in protecting data; complying with the provisions of data protection law; and in managing risks to college data.

3. SCOPE

This policy applies to:

- All data created or received in the course of college business in all formats, of any age. "Data" shall include personal and special category data; and also confidential and commercially sensitive data.
- Data held or transmitted in physical (including paper) and electronic formats.
- Data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone).

Who is affected by the policy:

- College staff (which includes contractors, temporary staff and anyone else who can access or use data, including personal and special categories of data, in their work for the college).
- Non-staff data subjects (these include, but are not confined to: prospective applicants; applicants to programmes and posts; current and former students; alumni; former employees; family members where emergency or next of kin contacts are held, members of the Board of Management and Edinburgh College committees, volunteers, potential and actual donors, customers, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

Where the policy applies:

- This policy applies to all locations from which college data is accessed, including home use and overseas.

4. OBJECTIVES

This policy sets out a framework of governance and accountability for data protection compliance across the college, with particular reference to personal and sensitive personal data (now called special category personal data) and the college's responsibilities for this under data protection legislation.

The Data Protection Policy forms part of the college's framework for Information Governance more broadly and should be read in conjunction with associated policies including the Information Security Policy and the IT Facilities Acceptable Use Policy. The Information Security Policy separately sets out the principles by which the college maintains:

- Confidentiality: protecting information from unauthorised access and disclosure;
- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion;
- Availability: ensuring that information and associated services are available to authorised users whenever and wherever required;
- Resilience: the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident.

4.1 Data Security and Classification:

Guidance on the formal classification of the different types of data processed by the college - and appropriate specific security arrangements for each class of data - will be outlined following the completion of the college's Records Management review.

However, the following general principle applies at all times to all data managed by the college, whether the data area personal and/or special category data; confidential business data; or commercially sensitive data:

- All college users of data must ensure that all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork shall be locked away when not in use;
- Portable devices (laptops, memory sticks, external hard drives) should not be left unattended;

Further information on the college's duty - and policy on - protecting personal and special category data is outlined in section 5.1.6 below.

5. LEGAL GOVERNANCE

The safe and secure management of information is integral to Edinburgh College's values (a trustworthy organisation); and a key enabler of effective business practice.

However, beyond this Edinburgh College must comply with data protection legislation ensuring the College is specifically protecting the privacy rights of individuals where their personal and special category data are concerned. These data protection laws require the college to protect personal information and control how it is used in accordance with the legal rights of data subjects – the individuals whose personal data is held. For comprehensive information on the range of data protection legislation to which the college is subject please contact the Information Management Team.

Under data protection laws the college is responsible for, and must be able to demonstrate compliance with, the following data protection principles as set down in the General Data Protection Regulation, and the Data Protection Act 2018, and outlined in the section below.

5.1 Data Protection Principles:

There are 6 Data Protection Principles. They are as follows:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

2. Personal data shall be collected only for specified explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ('purpose limitation').

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

4. Personal data processed shall be accurate and, where necessary, kept up to date ('accuracy').

5. Personal data shall be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed ('storage limitation').

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or

unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Edinburgh College must also meet the 'Accountability principle' which means the College is responsible for and must be able to demonstrate compliance with the six principles above. This principle compels the College to adopt policies and implement appropriate measures to ensure and demonstrate that the processing of personal data complies with privacy law. The College is required to maintain necessary documentation of all processing activities; implement appropriate security measures (technical and organisational); perform Data Protection Impact Assessments (DPIAs); comply with the requirement of prior notification/consultation with the regulator (where there are significant risks identified by a DPIA); and designate a Data Protection Officer (DPO).

Individuals (data subjects) have rights under data protection law, these rights are listed later on in this policy. The College has appropriate procedures in place to ensure these rights can be actioned if an individual makes a request.

5.1.1 **Principle 1**: Personal data shall be processed fairly, lawfully and transparently.

This means that Edinburgh College shall:

- Only collect and use personal data in accordance with the lawful conditions set down in data protection law and do not do anything in breach of any other laws;
- Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect;
- Inform people how we use their personal data and what their rights are (known as a privacy notice). This includes being clear, open and honest about how the College uses their data to meet the transparency requirements of the right to be informed (for further detail please see section about individuals' rights);
- Rely on an individual's consent, as the legal basis for processing their personal data, only where:
- We've obtained the data subject's specific, informed and freely given consent, and:

    - The individual has given consent, by a statement or a clear affirmative action (that we document);
    - The individual has the right to withdraw their consent at any time without detriment to their interests; and that it is as easy to withdraw consent as it is to provide it.

5.1.2 **Principle 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').

This means that Edinburgh College shall:

- Ensure that if we collect someone's personal data for one purpose (e.g. to provide advice on study skills), we will not reuse their data for a different purpose that the individual did not agree to or expect (e.g. to promote goods and services for an external supplier);
- Be clear in the privacy notice as to the specific purposes of processing and ensure that the data subjects are fully informed (for further information regarding right to be informed see section below on individuals rights);
- If the data is to be used for another purpose we will ensure that it is compatible with original purpose, or get the individual's specific consent for the new purpose.

5.1.3 **Principle 3**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

This means that Edinburgh College shall:

- Only collect personal data that is sufficient for the stated purpose;
- Relevant for that purpose (i.e. we will not collect personal data that is not necessary for the stated purpose);
- We will only collect the minimum data required, (i.e. we will not collect more personal data that is necessary for the purpose);
- Reduce risks of disclosure by pseudonymising personal data where possible;
- Anonymise personal data wherever necessary and appropriate, (e.g. when using it for statistical purposes), so that individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

5.1.4 **Principle 4**: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

This means that Edinburgh College shall:

- Take all reasonable steps to ensure personal data is not incorrect and have process in place to ensure that incorrect or misleading data is corrected or erased as soon as possible;
- The personal data will be updated where appropriate, (e.g. when informed of a change of address, our records will be updated accordingly);

- Ensure the accuracy of the personal data we create and record the source of that data (e.g. from data subject or from partner organisation);
- We have process in place to address an individual's right to rectification: how it is considered, actioned and recorded.

5.1.5 **Principle 5**: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');

This means that Edinburgh College shall:

- Only keep personal data for as long as necessary for the purpose it was collected for;
- Apply the College's records management policy and retention and disposal schedule in relation to all records and will regularly review the retention period for any records containing personal data;
- Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten';
- Destroy records securely in a manner appropriate to their format or anonymise the personal data when we no longer require it;
- Identify personal data that needs to be kept for public interest archiving, scientific or historical research or statistical purposes

5.1.6 **Principle 6:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

This means that Edinburgh College shall:

- Have appropriate organisational security measures in place to protect personal data, including an Information Security Policy and IT Facilities Acceptable Use Policy;
- Have appropriate technical security measures in place to protect personal data;
- Have appropriate physical and personnel security measures in place, (e.g. secure rooms where personal data is held);
- Control access to personal data so that staff, contractors and other people working in the College can only see the personal data that is necessary for them to fulfil their duties;
- Require all College staff, contractors, students and others who have access to personal data in the course of their work to complete data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles;

- Set and monitor compliance with security standards for the management of personal data as part of the College's framework of information governance policies and procedures;
- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from the College;
- Where transferring personal data to another country outside the European Union put in place appropriate agreements and auditable security controls to maintain privacy rights;
- Have a robust security incident reporting procedure in place to manage, investigate and, where applicable, report to the Information Commissioner's Office and data subjects affected;
- Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer shall liaise with the Information Commissioner's Office and report the breach, in line with regulatory requirements, within 72 hours of discovery. The Data Protection Officer shall also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

5.1.7 **Accountability:**

The accountability principle requires the College to take responsibility for what it does with personal data and how it complies with the data protection principles. The College must have the following required documentation and records in place in order to demonstrate compliance.

This includes the following:

- Records of Processing Activities. This will contain all the business functions of the College which collect personal data; the types of personal data collected; the source of the data; who (if any) it is shared with; the security measures in place to protect it; the retention and disposal of the data and the legal basis that it is collected for and the conditions for processing. This must be maintained and reviewed on a regular basis;
- Adopting and implementing data protection policies and procedures that demonstrate appropriate technical and organisational security measures are in place;
- Appointing a Data Protection Officer (DPO): the College DPO is Alice Wilson who can be contacted via the data protection mailbox DataProtection@edinburghcollege.ac.uk;
- Implementing a 'data protection by design and default' approach. This means that whenever a policy, process or system involves personal data that the College considers and builds in the appropriate safeguards to protect the personal data from the start;
- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate

privacy risks at each stage of every project or initiative involving processing personal data; and in managing upgrades or enhancements to systems and processes used to process personal data;

- Ensuring appropriate contracts are in place with any third party organisations who process personal data on the College's behalf and where the College shares personal data with other organisations that this is properly documented in a data sharing agreement (DSA);
- Recording and where appropriate reporting personal data breaches to the regulator (UK Information Commissioner's Office (ICO)) and if necessary the data subjects;
- The College will adhere to relevant codes of conduct and where applicable sign up to certification schemes.

The accountability principle is an ongoing obligation and the college shall regularly review (and where necessary update) documentation and risk assessments. Through meeting the accountability requirements the College shall continue to meet its values of being trustworthy, with individuals being assured that their personal information is secure.

5.2 Rights of Data Subjects (Individuals)

Data subjects have a number of rights under data protection law. These are:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

These rights are explained in further detail below. It's important to note that some rights have certain conditions that must be met for the rights to apply. When an individual makes any request to exercise their rights then the request must be sent to the data protection mailbox DataProtection@edinburghcollege.ac.uk and the Information Management team will process it accordingly. All requests must be answered within one month.

5.2.1 Right to be informed

This means that, at the point that we collect individuals' personal data, we will explain to them in a clear, concise and accessible way the following information:

- The name and contact details of our organisation;
- The name and contact details of the college and the Data Protection Officer (Alice Wilson);
- For what purposes we collect and use their personal data;
- What lawful conditions we rely on to process data for each purpose and how this affects their rights; Our obligations to protect their personal data;
- What personal data we collect (if the personal data is not obtained from the individual it relates to);
- The sources from which we obtain their data, where we have received the data from third parties;
- To whom we may disclose their data and why (e.g. sharing with accrediting bodies like the SQA);
- Which other countries we may we may send their data to, why we need to do this and what safeguards apply in each case;
- How long we intend to retain their data, and that it will be destroyed securely when we no longer require it;
- The rights available to individuals in respect of the processing and how to exercise their rights including:

    - The right to access;
    - The right to object;
    - The right to rectification;
    - The right to withdraw consent (when consent has been used);
    - The right to lodge a complaint with the regulator – the UK Information Commissioner's Office (ICO);

- Whether they need to provide data to meet a statutory or contractual requirement and if so, the consequences of not providing the data;
- Whether we use automated decision making, including profiling, and if so the impact on data subjects and their rights to object.

The College shall publish this information on its website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

Where we process personal data to keep people informed about college activities and events we will provide in each communication a simple way of opting out of further marketing communications.

In these ways the college shall provide accountability for our use of personal data and demonstrate that we will manage people's data in accordance with their rights and expectations.

5.2.2 The right of access

This means that individuals have the right to request access to their personal data that the College holds. Any individual may make such a request and receive a copy of their information free of charge and within one month of their request.

5.2.3 Right to rectification

This means that individuals have the right to have inaccurate personal data rectified and incomplete personal data completed. We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them, such as home addresses.

5.2.4 The right to erasure

This is commonly known as the right to be forgotten. It means that individuals can have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data.

5.2.5 The right to restrict processing

Individuals may restrict the processing of their personal data until a dispute about the data's accuracy (see 4.2.3) or use has been resolved, or when the College no longer needs to keep personal data but the data subject needs the data for a legal claim.

5.2.6 The right to data portability

This means that where a data subject has provided personal data to the College by consent or contract for automated processing they have the right to request a machine readable copy or have it sent to another data controller.

5.2.7 The right to object

All individuals have the right to object and prevent further processing of their data. This right is not absolute and requires certain conditions to be met. This includes:

- Where the College is processing personal data for direct marketing purposes an individual can object and the College must stop processing their data for marketing;
- Stop the College processing data obtained for online services such as social media, where consent for the processing was previously given by or on behalf of a child, who withdraws their consent;
- Object to decisions that affect them being taken solely by automated means;
- If the individual objects to processing which is carried out in the course of the College's legitimate interest or public interest unless the College can demonstrate compelling lawful grounds for continuing to process the individual's data.

5.2.8 Rights in relation to automated decision making and profiling

Automated individual decision-making means a decision is made solely by automated means and without any human intervention. Profiling is automating processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision making process. This type of decision making can only be carried out where the decision is necessary for the entry into or performance of a contract; authorised by law or based on the individual's explicit consent.

When the College processes personal data which involves automated decision making or profiling then it's important that the College does the following:

- Provide the individual with information about the processing;
- Provide a simple way for them to request human intervention or challenge a decision;
- Carry out checks to ensure that the systems are working properly as intended.

6. RISKS OF NON COMPLIANCE

Misuse of personal data, through loss, disclosure or failure to comply with the data protection principles and the rights of data subjects, may result in significant legal, financial and reputational damage. This may include penalties of up to €20m or 4% of worldwide annual turnover of serious breaches of the law, claims for compensation and loss of reputation. It's important to note that in the event of personal or special category data breach individuals may claim compensation for damages caused by the breach.

Non-compliance with the data protection principles, or any concerns over data protection, must immediately be reported to DataProtection@Edinburghcollege.ac.uk

7. AUTHORITY

This policy is issued under the authority of the Chief Operating Officer who is also responsible for its interpretation and enforcement, and who may also delegate such authority to other people.

Users must comply with any reasonable written or verbal instruction issued by people with delegated authority in support of this policy. If users feel that any such instructions are unreasonable or are not in support of these regulations, users may appeal to the Chief Operating Officer within Edinburgh College or contact the college's Data Protection Officer, Alice Wilson.

8. LINES OF RESPONSIBILITY

8.1.1 All users of college information are responsible for:

- Completing relevant training and awareness activities provided by the college to support compliance with this policy;
- Taking all necessary steps to ensure that no breaches of information security result from their actions (taking into account data security principles in 4.1);
- Reporting all suspected information security breaches or incidents immediately to DataProtection@edinburghcollege.ac.uk so that appropriate action can be taken to minimise harm;
- Complying with the data protection principles set out in in section 5;

- Informing the college of any changes to the information that they have provided to the college in connection with their employment or studies, for instance, changes of address or bank account details.

8.1.2 The Principal & Chief Executive

As the Chief Executive Officer of the College, the Principal has ultimate accountability for the college's compliance with data protection law.

8.1.3 Chief Operating Officer

The Chief Operating Officer has senior management accountability for data protection, reporting to the Principal & Chief Executive and the Audit and Risk Assurance Committee on relevant risks and issues.

8.1.4 The Information Management Team and Data Protection Officer (DPO)

The Information Management team and the Data Protection Officer (DPO) are responsible for ensuring that the College complies with data protection law; the principles therein; and ensuring that procedures are in place for individuals to exercise any of their rights. The Information Management Team and DPO are responsible for investigating reported data breaches.

8.1.5 Heads of Functions

Heads of Functions are responsible for ensuring that all staff manage their devolved responsibilities for compliance with this policy.

9. POLICY MONITORING AND EVALUATION

The Head of Corporate Development will set up management processes to monitor compliance with this policy and will report to the Chief Operating Officer, Information Management Group, and Audit and Risk Assurance Committee any breaches of this policy which present data protection risks and issues, and agree actions to address these.

The terms of this policy must be observed at all times. Any failure to comply with the terms of this policy may lead to disciplinary action being taken against the user in accordance with the college disciplinary policy and/or legal proceedings.

The type of disciplinary action taken will be dependent on the seriousness of the issue. Factors that will be taken into account include:

- Breaches of confidentiality, security and the law;
- Damage to the college's reputation;
- Damage to data subjects' rights and/or freedoms;
- Creation of a hostile working environment;

The College reserves the right to:

- Pass information to the relevant statutory authorities;
- Withdraw a user's access to any IT system, including internet services;

The above list of sanctions is not exhaustive and may be altered or augmented by the college depending on the nature of the incident.

10. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

This policy should also be read in conjunction with the College's Disciplinary policies and procedures; the college Information Security Policy; and the IT Facilities Acceptable Use Policy.

These policies and procedures are reviewed and updated as necessary to maintain an effective Information Governance Management System to meet the College's business needs and legal obligations.

Legal requirements and external standards

Data protection is subject to U.K. and European law and other relevant law in all jurisdictions in which the College operates.

All current UK Legislation is published at http://www.legislation.gov.uk/

The legislation listed below includes the key legislation on which this policy is based. It is important to note this is not an exhaustive list of legislation governing the college's wider operations.

Data Protection Act 2018	Malicious Communications Act 1988
EU General Data Protection Regulation (GDPR)	Privacy and Electronic Communications Regulations (PECR)
Computer Misuse Act 1990	Copyrights, Designs, Patents Act 1988
Trade Marks Act 1994	Freedom of Information Act (Scotland) 2002
Sex Discrimination Act 1986	Race Relations Act 1976, 1999
Defamation Action 1996	

11. FURTHER HELP AND ADVICE

For further information and advice about this policy contact:

Email: DataProtection@edinburghcollege.ac.uk
Telephone: 0131 297 8663

12. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
1.0	28/06/2018	Senior Management Group	Approval of policy by Senior Management Group
1.1	03/07/2018	Nick Murton	Addition of Policy Version and History; and document control header.
1.2	01/08/2018	Nick Murton	Addition of EQIA data; correction of SMG approval date
1.3	01/08/2018	Nick Murton	Footer updated

ANNEX A - DEFINITIONS IN DATA PROTECTION

The following provides a definition of the terminology used in this policy in relation to data protection law.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data (fingerprint).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data controller means the organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor means the organisation which processes personal data on behalf of the data controller. *If an organisation is a data processor there are specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.*

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; (Art 4(6)).

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample form the natural person in question (Art 4(13)).

Personal data means any information relating to an identifiable person (**data subject**); who can be directly or indirectly identified in particular by reference to an identifier. This definition is wide a means that a wide range of personal identifiers constitute personal data. This includes name, identification number (e.g. NI Number), location data, online identifier (IP address) which reflects the changes in technology and the way that organisations collect information about individuals. It also includes information relating to factors specific to the physical, physiological genetic, mental, economic, cultural or social identity of that individual.

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 (Art 4(12)).

Processing means any operation or set of operations which is performed on personal data or on sets of personal data. Processing occurs whether it is electronic or physical records, it includes: 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. So even if data is held in a server but not used this is still processing.

Profiling means 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.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be identifiable without the use of additional information, provided. The additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data identifiable unless the additional information (e.g. use of a key code).

Recipient means a natural or legal person, public authority agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. (Art4(9)).

Restriction of processing mean the marking of stored personal data with the aim of limiting their processing in the future.

Special category data (formerly known as sensitive personal data) means personal data which identifies an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. This data requires extra safeguards to protect it from unauthorised use, disclosure etc as it is considered that this information can have a higher impact on the rights and freedoms of an individual. Criminal records and convictions information is not under this category of data but should also be handled with extra safeguards due to the sensitivity of the information.

Territorial Scope: Data protection law applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Third party means a natural or legal person, public authority, agency or boy other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data; (Art4(10)).