South Eastern Health and Social Care Trust

Policy Code: SET/Gen (48) 2019

SOUTH EASTERN TRUST

Title:	**Data Protection Policy Statement**			
Author(s)	**Head of Information Governance & Directorate Support**			
Ownership:	**South Eastern Trust**			
Approval by:	**Information Governance Steering Committee**		**Approval date:**	**September 2018**
Operational Date:	**April 2019**		**Next Review:**	**April 2024**
Version No.	**4.0**	**Supercedes**	**SET/Gen (146) 2016**	
Key word/s	**Data, information, protection, regulation, legislation, asset, Caldicott**			
Links to other policies	**Evidence Base: References at end of policy**			

1.0 INTRODUCTION/PURPOSE OF POLICY

1.1 The South Eastern HSC Trust (hereafter referred to as the Trust) needs to collect, use and process personal data, including *sensitive data,* about the people with whom it deals. These people include current, past and prospective patients, clients, staff, service providers and suppliers. In addition the Trust is required by law to collect and use certain types of information to comply with requirements of government departments for example medical records, social service data, public health data, statistics, business data etc. This information must be managed within a framework which provides optimum protection for patients, clients, staff & customers alike – i.e. in compliance with current legislation, the Data Protection Act 2018, and extending beyond this to take account of Caldicott recommendations (see Appendix 2) and the general duty of confidentiality.

1.2 Through its day to day operations the Trust is required to collect and hold certain types of personal data including information about people with whom it interacts in order to operate.

1.3 The legal requirement for the Trust and its staff to treat personal information confidentially and hold it securely is set out in the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Protection Act 2018. The introduction of this new data protection legislation in 2018 will bring all EU countries into line with previously unforeseen ways that data is now used. The legislation places the concept of confidentiality within a legal framework and imposes both corporate and individual responsibilities.

1.4 Purpose

1.4.1 The lawful and correct handling of personal data by the staff of the Trust is crucial to the success and maintenance of confidence between the Trust and those with whom it interacts, both internally

and externally. The legislation makes provision for the regulation of the processing of personal information relating to living individuals, including the obtaining, holding, use, disclosure and destruction of such information.

1.4.2 This policy has been introduced with the aim of empowering managers to be proactive in relation to the protection of personal information in their workplace.

1.4.3 This Policy should be read in conjunction with the following policies:-

- Information Governance Strategy
- Records Management Policy
- Freedom of Information
- Information Communication & Technology (ICT) Strategy
- Securing Records for the Purposes of Investigations

1.4.4 In addition, the Trust adheres to and has implemented the following Department of Health (DOH) (formerly Department of Social Services & Public Safety) Guidelines and Protocols:-

- Protocol for Sharing Service User Information for Secondary Purposes 2011
- Good Management: Good Records, December 2011 (GMGR [under revision])
- Code of Practice on Protecting the Confidentiality of Service User Information, January 2012

1.5 Objectives

1.5.1 The Trust needs to collect and use certain types of information about people with whom it interacts in order to operate. These include current, past and prospective employees, suppliers, clients, service users, patients and others with whom it communicates.

1.5.2 In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments or other bodies (e.g. Police Service of Northern Ireland). This personal information must be dealt with properly regardless of how it is collected, recorded and used – whether on paper, in a computer or recorded on other material – there are safeguards to ensure this in the GDPR and the Data Protection Act 2018.

1.5.3 The lawful and correct treatment of personal information by the Trust is regarded as very important to the success of our operation and to maintaining confidence with those the Trust deals with. To this end, the Trust fully endorses and will adhere to the principles of data protection as enumerated in the GDPR (see Appendix 1). The recently revised Caldicott principles (see Appendix 2) also provide very practical standards in relation to handling personal information. It

should be noted that the duty to share information can be as important as the duty to protect patient confidentiality.

2.0 SCOPE OF THE POLICY

2.1 This policy will apply to all staff. It is vital that this and the supporting policy and procedures are implemented and adhered to by all existing and new staff, including for example: admin (including agency) students, trainees, individuals on placement and volunteers. This also includes those contracted in temporarily, such as GPs and locums, and anyone reviewing records for the purpose of audit e.g. RQIA.

2.2 The GDPR covers all personal information handled within the Trust relating to **living** individuals, including that held on paper, electronic, digital, archival and back up media and being processed for any purpose i.e. research, audit, provision of care etc. This also includes all personal information that is appropriately removed/transferred/viewed by staff using portable media or remote access devices when working off-site or home.

2.3 It should be noted that the Freedom of Information Act is a separate piece of legislation which gives the public a right of access to types of 'recorded' information held by Public Authorities; it does not in general apply to personal information. For further information in relation to FOI refer to the Trust's Freedom Of Information Policy.

3.0 ROLES/RESPONSIBILITIES

3.1 The Trust and any organisation carrying out functions on its behalf, have a legal obligation to safeguard personal information and a duty to support staff exercising ethical standards of confidentiality. In order to fulfil these responsibilities, the Trust will ensure that this policy is disseminated to all staff, that it is understood and adhered to. Organisations carrying out functions on their behalf of the Trust should also provide the Trust with assurances that they and their staff comply fully with the GDPR.

3.2 The Trust Chief Executive has nominated joint responsibility for the role of Data Guardian to the Medical Director and the Executive Director of Social Work. The Guardian actively supports work to facilitate and enable information sharing and advises on options for lawful and ethical processing of information as required.

3.3 The Information Governance Steering Committee (IGSC) is chaired by the Director of Human Resources and Corporate Affairs and has responsibility for monitoring compliance and effectiveness of information and personal data security within the Trust.

3.4 The Chief Executive's and Directors' Responsibilities

Ultimately, responsibility for all aspects of processing personal information lies with the Chief Executive. However, responsibility is delegated to individual Directors within each Directorate for personal information within that area. Therefore, Directors have specific responsibilities to:

- Satisfy themselves that this policy and associated policies and procedures are implemented for their area of responsibility;
- Ensure personal information is used only for purposes for which it was obtained.

3.5 The Senior Information Risk Owners (SIRO) Responsibilities

The SIRO as a Director of the Trust is familiar with information risks and is responsible for the management of information risk at Board level. The Director of Human Resources & Corporate Affairs is responsible for this within the Trust and therefore has a key role in ensuring that the Trust complies with its legal responsibilities in this regard.

3.6 The Information Asset Owner (IAO) Responsibilities

The role of an IAO is to understand what information is held , what is added and what is removed, how information is moved and who has access and why. As a result a key part of their role is to understand and address risks to information and to lead and foster a culture that values, protects and uses information for the public good. This role is undertaken by all Assistant Directors within the Trust.

3.7 Managers' Responsibilities

Managers have specific responsibilities in the implementation of this policy and in monitoring compliance with it. This includes:

- The implementation of the general procedures within their departments;
- The preparation and implementation of specific departmental procedures, where necessary and appropriate;
- Ensuring that all staff receive mandatory training in the protection of personal information; and are familiar with the content of this policy;
- Monitoring adherence to procedures on a day-to-day basis and reporting any data breaches to the Information Governance Department and relevant IAO in a timely manner and,
- Ensuring that staff receive mandatory initial data protection training and refresher training every 3 years.

3.8 Individual Members of Staff Responsibilities

All Trust staff (including students, agency staff, trainees and individuals on placement) have a responsibility to abide by the principles contained within this document and adhere to the associated procedural guidelines. These documents are complementary to the ethical duty of confidence contained within the professional regulations for health and social care professionals. Staff should be aware that failure to adhere to the guidance given in this policy and related procedures could result in them being personally liable under GDPR and may also result in disciplinary action. This could ultimately lead to criminal proceedings by the PSNI or action from the ICO. Staff should ensure that they receive initial data protection training and refresher training every **three** years.

4.0 KEY POLICY PRINCIPLES

4.1 Definitions – See Appendix 3 for key definitions within the legislation.

4.2 The main focus of this policy statement is on providing guidance in relation to the protection, sharing and disclosure of patient/client/staff information, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to all Trust staff.

4.3 Every citizen needs to feel confident that information about their Health & Social Care is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the Trust should see information governance as part of their responsibility.

4.4 All users of personal data within the Trust have a responsibility to ensure that they process the data in accordance with the six data protection principles taken from the GDPR and summarised in Appendix 1. As part of the legislation the Trust shall be responsible for, and be able to demonstrate, compliance with the principles. There is significantly more accountability required with the GDPR legislation.

4.5 Obtaining Personal Information

4.5.1 Personal information should not be collected or used unless there is justification, both legally and practically, for doing so. A clear purpose should be documented.

4.5.2 Individuals should be told how their personal information might be used before they are asked to provide it.

4.5.3 The Trust should provide guidance on how personal information is being processed i.e. through Fair Processing Notices (FPNs). As well as overarching privacy notices, individual services may also wish to ensure patients/clients are aware of how their information will be processed in local leaflets and guidance. FPNs are available on the Information Governance IConnect site.

4.5.4 Where a particular use of information is not essential, the explicit consent of individuals to the use of their personal information will be sought, in advance of their being asked to provide it. There should be a legal basis for the processing of all information within the Trust. Refer to Articles 6 and 9 of GDPR (Appendix 4).

4.5.5 Data Privacy Impact Assessments (DPIAs) should be undertaken for new projects within the Trust that involve the use of personal data. DPIAs are a tool that can be used to identify and reduce the privacy risks of projects. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help to design more efficient and effective processes for handling personal data. DPIAs are **mandatory** where there processing is ‘a high risk for the rights and freedoms of individuals’. The DAA template is available on the Information Governance IConnect site.

4.6 Records and Record Keeping

4.6.1 Personal information should be adequate, relevant and not excessive for the reason(s) for which it is collected or used

4.6.2 Personal information should be accurate and kept up to date and,

4.6.3 All records should be clear, relevant and concise and indicate the identity of any persons who have made an entry in them. The use of abbreviations and jargon should be avoided unless they are from agreed lists.

4.6.4 Refer to the Trusts Records Management Policy for further information, available on the Trust's IConnect site under Policy.

4.7 Security of Personal Information

4.7.1 Appropriate measures must be taken against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (See the ICT Security Policy for further information) and,

4.7.2 To avoid unauthorised disclosure care must be taken to site PC's and terminals so that they are not visible except to authorised people. Care must be taken to ensure that manual records, files and printouts etc. are not left where they can be accessed by unauthorised staff.

4.8 Access to Personal Information

4.8.1 Requests for access to personal information should be dealt with in line with current Trust procedures, whether made by the individual, their representative, or person with parental responsibility and in keeping with the requirements of GDPR. For further advice and guidance on how to access personal information contact the Information Governance Department.

- Staff should only access data that is relevant for their area of work, Trust systems may be audited to identify usage. Staff should never use their access to Trust systems in order to access their own records or those on family/friends or anyone not connected to their role in work; the subject access process is the appropriate route to obtain this information. Inappropriate access to personal data can result in disciplinary action, potentially defined as gross misconduct specifically, but not restricted to, breaches of confidentiality. The Trust must report these breaches to the ICO who will undertake a separate investigation which could lead to prosecutions.

4.9 Sharing Personal Information

4.9.1 Access by anyone to personal information should be controlled and information released on a 'need to know' basis and in compliance with the legislation or other legitimate expressed instruction. Unless there

is an essential purpose or legal requirement only anonymised and/or aggregated information should be released

4.9.2 Any personal information given or received in confidence for one purpose MUST NOT be used for a different purpose, or passed to anyone else without the knowledge and consent of the individual concerned (or, if appropriate their representative)

4.9.3 The disclosure of personal information should be restricted to only as much information as is necessary for the purpose and,

4.9.4 In cases where a bulk transfer of person-identifiable information is to be shared with an external body for secondary purposes i.e. not direct patient care, it will be necessary to complete the Trust's Data Access Agreement form. Personal data is where an individual can be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the data controller i.e. the Trust.

4.9.5 A data access agreement ensures appropriate procedures have been adhered to and that there is authorisation for the sharing of data. A copy of the Data Access Agreement form is available on the Information Governance IConnect site.

4.9.6 The wishes of an individual to withhold or restrict the transfer of his/her personal information should be respected. However, this does not override the Trust's responsibility, in designated circumstances, to provide information for legal or statutory purposes or to protect the public.

4.10 Movement and Transport of Personal Information

4.10.1 Paper-based files containing personal information will only be removed from storage areas when necessary and their location should be tracked at all times.

4.10.2 Personal information will be transferred by secured means and only to places where the Trust is satisfied that it will receive an adequate level of protection. See Transferring Personal Information Policy and Procedures.

4.11 Retention and Destruction of Personal Information

4.11.1 Personal information will not be kept longer than is necessary for the reason(s) for which it was collected.

4.11.2 Records containing personal information will be destroyed on a timely basis and in line with the Trust's Policy on the Retention and Disposal of Records. See Trust Retention and Disposal Schedule available at the Department of Health (DOH) website.

4.11.3 Once identified as appropriate for destruction, personal information will be disposed of in such a manner that it is not possible to reconstitute the data.

4.11.4 Confidential waste should be used for the routine disposal of personal identifiable data.

4.12 Use of Technology

4.12.1 Technology will be used in such a way as to assist with the protection of data e.g. use of passwords, encryption etc.

4.12.2 The Trust will encourage new ways of working with the Information Communication Technology (ICT) Department to maximise the secure access, storage and transfer of data.

4.13 Data Breaches

4.13.1 The legislation requires organisations to report data breaches within 72 hours of being 'aware' of a breach. Failure to do so may result in the Information Commissioners Office (ICO) taking further action.

4.13.2 Any data breach must be recorded on an IR1/Datix and communicated to the IAO of the Service area and the Information Governance Department. The discoverer must verbally confirm with the IAO and Information Governance department that they are aware of the breach: sending an email is not sufficient.

4.14 Training and Communication

4.14.1 Staff should understand their responsibilities with respect to the proper handling of data through attendance at either: - HR induction, or by completing the e-learning module available on the Trust intranet site. Training must be refreshed every 3 years.

4.14.2 A range of training courses are made available through the Trust's learning and development module of the Human Resources, Payroll, Travel and Subsistence System (HRPTS).

4.15 Development of Policies & Procedures

4.15.1 A range of policies have been developed by the Information Governance Department to assist with complying with the Data Protection legislation. Further policies will be developed as necessary.

5.0 IMPLEMENTATION OF PROCECURE

5.1 Dissemination

5.1.1 This policy will be made available to all staff via the intranet. For those staff who do not have network access, managers are required to bring this policy to their attention.

5.2 Resources

5.2.1 This policy will be available on I-Connect and incorporated in the Information Governance Bulletins. A staff booklet entitled 'Employees Guide to Handling Information' is available to all new staff as a precursor to training, or from the Information Governance Team for existing staff.

5.2.2 The Trust has currently over 700 separate digital information systems. The ability to audit these systems varies from system to system. Likewise there are differences in the ability to delete information from systems. Without significant investment information may be held for longer than is required. Adequate auditing and deletion capabilities must be built into the specification of all new information systems, in accordance with GMGR.

5.3 Exceptions

5.3.1 This procedure applies to all areas of the Trust. There are no exceptions.

6.0 MONITORING

6.1 This procedure will be reviewed every 3 years (or sooner if new legislation, codes of practice or national standards are introduced).

6.2 It is the responsibility of line managers to monitor the completion and review of staff training and information governance incident reporting and investigation. Other specific monitoring responsibilities will be under the remit of the Information Governance Sub Committee.

7.0 REFERENCES

The Data Protection Act, 2018 available at :-
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm
General Data Protection Regulation (EU) available at :-
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
DHSSPS *Good Management: Good Records,* DHSSPS available at:-
https://www.health-ni.gov.uk/topics/good-management-good-records
DHSSPS & HSC *Protocol for Sharing Service User Information for Secondary Purposes* available at:-
http://setintranet/filestore/publications/dhssps___hsc_protocol_for_sharing_service_user_information_for_secondary_purposes__final__pdf_.pdf
DHSSPS *Code of Practice for Protecting the Confidentiality of Service User Information*, 2012 available at:-
http://setintranet/filestore/publications/Code_of_Pratice_on_Protecting_the_Confidentiality_of_Service_User_Information.pdf
Information Governance i-connect site
http://setintranet/departments/information_governance/
Information Commissioners Office website available at : - https://ico.org.uk/

8.0 CONSULTANTION PROCESS

The revision of this Policy has been consulted via the Information Governance Steering Committee and Senior Managers within the Risk Management & Governance Directorate.

9.0 APPENDICES

Appendix 1 – Six Principles of the Data Protection Act.
Appendix 2 – Caldicott Principles
Appendix 3 – Definitions
Appendix 4 – Articles 6 and 9 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

10.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.
The outcome of the Equality screening for this policy is:

Major impact ☐

Minor impact ☐

No impact. ✓

SIGNATORIES

(Policy – Guidance should be signed off by the author of the policy and the identified responsible director).

Policy Name	Author Endorsement	Modified	Modified By
Data Protection 2019	Yes	20/03/2019 04:05 PM	McAree, Lynda

Policy Name	Approval	Modified	Modified By
Data Protection 2019	Endorsed	25/03/2019 02:28 PM	Weir, Myra

Appendix 1

General Data Protection Regulation Principles

The GDPR principles require that personal information:

Article 5 of the GDPR requires that data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) 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;

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject; and

(f) 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."

Appendix 2

Caldicott Principles

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix 3

Key Policy Definitions

Terms	Definition
GDPR	The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. It came into effect on 25 May 2018.
Data Protection Act 2018	*An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relation to information; to make provision for a direct marketing code of conduct; and for connected purposes.*
Data Controller	A controller determines the purposes and means of processing personal data.
Data Processor	A processor is responsible for processing personal data on behalf of a controller.
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. This definition provides a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
Special Categories of Personal Data **Previously referred to as Sensitive Data**	The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).
Data Privacy Impact Assessments	Data Privacy Impact Assessments (DPIAs) are a tool which can help organisations

	identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Appendix 4

Lawful Basis for Processing – Article 6 and Article 9 GDPR

Article 6
Lawfulness of Processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

(b) 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;

(c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;

(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or
(b) Member State law to which the controller is subject.
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing **for a purpose other than that for which the personal data have been collected** is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic

society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, **take into account**, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 9
Processing of special categories of personal data

1. Processing of personal data 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 **shall be prohibited**.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

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

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing **is necessary for reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services **on the basis of Union or Member State law or pursuant to contract** with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.