DATA PROTECTION POLICY

Published: March 2010

Last Reviewed: April 2018

Next Review Due: April 2019

Contents List

Appendices

1. Introduction

1.1 The Northern Ireland Local Government Officers' Superannuation Committee (NILGOSC) is a non-departmental public body sponsored by the Department for Communities, established on 1 April 1950 by the Local Government (Superannuation) Act 1950, to administer and maintain a fund providing pension benefits for employees of local authorities and other admitted bodies.

1.2 NILGOSC is a Data Controller under the EU General Data Protection Regulations (GDPR) and UK data protection legislation (from this point on collectively referred to as data protection legislation) as it collects, stores and controls how personal information relating to its members is managed. Consequently, it is required to hold, manage and process any personal data fairly, lawfully and in accordance with relevant data protection legislation.

1.3 NILGOSC takes its responsibilities as a data controller very seriously and is committed to complying with its statutory obligations under data protection legislation

2. Purpose

2.1 NILGOSC holds a significant amount of personal data, mainly belonging to Scheme members and beneficiaries, staff and Committee members. The purpose of this policy is to define NILGOSC's responsibilities under data protection legislation and to provide assurance that data is managed in compliance with statutory obligations.

2.2 This policy is designed to give Scheme members and beneficiaries an overview of how NILGOSC complies with data protection legislation in our working practices. It is also intended to provide an overview to staff of how data protection legislation should be applied to inform their decisions and day to day work by providing a legal background to the processing of personal data.

2.3 NILGOSC aims to achieve best practice standards in managing its information by adhering to best practice guidelines. This policy sets out the standards which NILGOSC applies when managing personal data, in order to ensure protection of our Scheme members and beneficiaries, staff and Committee members.

3. Scope

3.1 This policy applies to all staff, Committee members, employing authorities, contractors and partner agencies who:

- Process personal data as part of their role or on behalf of NILGOSC (including contracted service providers)
- Have access to NILGOSC's systems for the purposes of maintenance and/or service provision in line with a contracted duty
- Have access to NILGOSC premises where personal data is stored

3.2 Staff should read and apply this policy in conjunction with the Data Protection Procedures and Data Protection Quick Guide. In addition to these specific data protection policies and procedures, the following internal policies and guidance aim to maintain the confidentiality, integrity and availability of the personal data which is held by NILGOSC:

i. Retention & Disposal Schedule
ii. Information Security Policy
iii. Information Risk Policy
iv. Freedom of Information Policy and Procedures
v. Secure Desk Guidance

All of the above policies and procedures are available on the Staff Intranet.

4. Legislative Framework

4.1 The GDPR replaces the EU Data Protection Directive (95/46/EC) and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. The GDPR has broadened the data protection legislation and the framework of rights and duties designed to safeguard personal data.

4.2 The General Data Protection Regulation (GDPR) came into force on 25 May 2018 and will be directly applicable to all member states without the need for implementing national legislation. The UK Data Protection Bill is anticipated for enactment in 2018. The new Data Protection Act will effectively implement the GDPR and reiterate the privacy policies enshrined in EU Regulation. It will also clarify how the UK will apply statutory controls to areas of the GDPR where Member States have been given some flexibility i.e. the derogations.

4.3 The Freedom of Information Act 2000 remains in force and despite explicit reference to the Data Protection Act 1998, it will interplay with the GDPR and the new UK Data Protection Act once enacted in the UK.

4.4 The effective implementation of this policy is critical to ensuring NILGOSC's compliance with the legislative requirements governing personal data and privacy, namely the GDPR, UK data protection legislation and the Human Rights Act (1998).

4.5 Compliance with the DPA is monitored by the Information Commissioner's Office (ICO), an independent authority which has the power to take action against individuals or organisations which do not comply with the DPA. These powers include criminal prosecution, non-criminal enforcement, including issuing undertakings and enforcement notices, and audit. The ICO also has the power to serve a monetary penalty notice on a data controller, up to the value of €20m or 4% of global annual turnover.

4.6 The following legislation, international standards and Government requirements are also applicable:

- Freedom of Information Act (2000)
- Environmental Information Regulations (1992) & Environmental Information (Amendment) Regulations (1998)
- ISO 15489 -1 and ISO 15489 -2 Information and Documentation - Records Management
- ISO 27001- Information technology - Security techniques - Information Security Management Systems - Requirements
- Data Handling Procedures in Government: Final Report, Cabinet Office, June 2008
- HMG Security Policy Framework, Cabinet Office, July 2014
- Privacy and Electronic Communications (EC Directive) Regulations 2003

5. Notification

5.1 As a data controller, NILGOSC is registered with the ICO. Registration is a statutory requirement and every organisation must notify the ICO of the data they hold and the purpose for processing, for inclusion in the Data Protection Register. This notification must be renewed on an annual basis. Failure to do so is a criminal offence.

5.2 NILGOSC's Data Protection registration number is Z5698603. The register entry notes that personal data is held by NILGOSC in its capacity as "Trustees of a Pension Scheme"1.

6. Definitions

6.1 Some of the common definitions used in this Policy and the Data Protection Procedures are set out below:

6.2 ***Data*** can be factual information, such as names and addresses, or it can be expressions of opinion or intention and can occur in any format, e.g. Word documents, paper files, databases, spreadsheets, e-mails, microfilm, etc. Data is information which is:

- Processed on computer and/or in manual form;
- Recorded with the intention of processing on computer or manually;
- Recorded and kept electronically or manually; or
- Recorded information held by NILGOSC as a public authority, which does not fall within the above definitions.

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

6.4 ***Sensitive personal data*** means personal data consisting of information which may include any of the following: racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning natural person's sex life or sexual orientation.

6.5 ***Processing*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction erasure or destruction.

[1] This is a standard "Nature of work" description used by the Information Commissioner's Office for registration purposes.

6.6 ***Data controller*** means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. NILGOSC is the data controller for the personal data it holds, or which is processed under its instructions.

6.7 ***Data subject*** means any information relating to an identified or identifiable natural person. For NILGOSC this includes Scheme members, their partners and dependants, staff and Committee members.

6.8 ***Information Security Officer (ISO) –*** is the person within the organisation that is responsible for the development and implementation of information security policies to protect the organisation's information assets. Information Security relates to more than personal data.

6.9 ***Data Protection Officer (DPO) -*** is the designated person within an organisation that has responsibility for ensuring legal compliance with GDPR, relating to personal data. The DPO for NILGOSC is the Governance Manager.

7. Categories of Individuals

In its role as administrator of the Local Government Pension Scheme (Northern Ireland), NILGOSC categorises its membership into the following profiles:

7.1 ***Members****:* Active Members, Deferred Members, Pensioner Members. NILGOSC is a single data controller for these categories of members.

7.2 ***Beneficiaries:*** Beneficiary Pensioners. NILGOSC is the data controller for these members.

7.3 ***Other Third Party Data:*** NILGOSC may hold information relating to a members' next of kin, e.g.: nomination form. The Scheme is a data controller for these persons and holds the information under Schedule 1(16) of the Data Protection Bill/Act, as the holding of the information is necessary for the purpose of making a determination in connection with eligibility for pension benefits.

8. Categories of Data

NILGOSC has identified that it holds data in the following distinct categories:

8.1 ***Personal Data:*** This relates to any information not classed as special category data.

8.2 ***Special Categories:*** As defined in the GDPR, this relates to sensitive personal information and may relate to Scheme members and beneficiaries, staff or Committee members. This particularly relates to member ill health retirement applications and NILGOSC's assessment of their entitlement to such benefits in line with Scheme Regulations.

8.3 ***Pensions Data:*** This relates to previous pension benefits accrued, potentially with another Scheme, which requires consideration when assessing entitlement.

8.4 ***Employer Data:*** This is information that NILGOSC may hold for Employing Authorities in the Scheme, for example individual officer contact details.

9. Overseas Data Transfer

NILGOSC has a number of overseas members who reside in countries other than the UK. NILGOSC does not transfer data relating to overseas members to anyone other than the individual.

10. The Data Protection Principles

10.1 The GDPR details six key principles which determine how personal data must be processed. In accordance with these principles, NILGOSC will ensure that:

1. Personal data is processed fairly and lawfully and in a transparent manner in relation to the data subject.

2. Personal data is collected for specified, explicit and legitimate purposes, and is not further processed in any manner incompatible with that purpose.

3. Personal data is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

4. Personal data is accurate and, where necessary, kept up to date. NILGOSC will take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Personal data processed for any purpose is 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.

6. 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.

GDPR also introduces a new accountability principle that requires organisations to be responsible for, and be able to demonstrate compliance with, the above processing principles.

10.2 NILGOSC undertook a data mapping exercise to identify all the categories of personal data that it processes on behalf of its Scheme members and beneficiaries, staff and Committee Members. This was used to develop a Record of Processing Activities (RoPA), which details the categories of data that NILGOSC processes, the legal basis for processing that data and who the data is shared with. This RoPA will be subject to regular review and update on an ongoing basis to ensure compliance with the above principles.

10.3 NILGOSC has published Privacy Notices for Scheme members and beneficiaries, staff, Committee Members and applicants to provide full transparency on the information that it holds, the legal basis for holding the data, who the data is shared with and how long the data is retained. These Privacy Notices are available from the NILGOSC website at http://www.nilgosc.org.uk/data-protection.

10.4 NILGOSC will ensure that the processing of personal data and special categories of personal data complies with the conditions set out in Articles 6 and 9 of GDPR, provided at Appendix A and Appendix B respectively.

11. Individuals' Rights

One of the key obligations for data controllers who manage and control individuals' data is to ensure the individual is informed about their rights, which gives them control over how their information is used and by whom. These rights are detailed as below:

a) *The right to be informed*

This is the right to know how information is used and who it will be shared with. NILGOSC will publish on its website a Privacy Notice which outlines what personal information it will gold, who it will share it with and for how long the information will be held. Should an individual feel that the information supplied in the Privacy Notice is inadequate or that it doesn't inform them about how their information is used by NILGOSC, staff should liaise with the DPO for more information and guidance.

b) *The right of access*

This is an individual's right to obtain:

i) confirmation that data is being processed and how it is being processed
ii) access to personal data
iii) access to policies and information held by NILGOSC about how it uses data.

This right, commonly referred to as subject access, enables individuals to verify that the Scheme is using data appropriately as well as providing access to obtain copies of information it holds. Individuals are entitled to see the information held and can request a copy in writing by post or by emailing governance@nilgosc.org.uk.

c) *The right to rectification*

Individuals have a right to have information amended or rectified if they believe it is inaccurate or incomplete. If NILGOSC agrees to rectify data and it has disclosed the personal data to others, each recipient of the data must be contacted to inform them of the rectification or completion of the personal data, unless this is impossible or involves a disproportionate effort.

d) *The right to erasure/The right to be forgotten*

This right allows individuals to request an organisation to delete any or all information about them. However, the 'right to erasure' does not provide an absolute 'right to be forgotten'.

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

(a) where personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
(b) When the individual withdraws consent
(c) When the individual objects to processing and there is no overriding legitimate interest for continuing the processing
(d) The personal data was unlawfully processed (i.e. otherwise in breach of data protection legislation)
(e) The personal data has to be erased in order to comply with a legal

obligation.

NILGOSC, in providing statutory duties under the Scheme Regulations, has determined that it cannot permanently delete a member's record. Should a member transfer out of the scheme, NILGOSC will retain a basic record confirming the member's name, contact details, date of birth and National Insurance number details, but it will endeavor to delete any other information including any documents relating to the member. The basic member details are required to be retained to enable NILGOSC to comply with statutory and legal obligations such as fraud prevention and GMP reconciliation. Particular weight should be given to any request for erasure of data collected from a data subject who is either a child, or provided consent at the time of being a child.

If NILGOSC erases data, it should inform any other organisation to whom the data has been disclosed unless this proves impossible or involves disproportionate effort. If requested, NILGOSC must inform the individuals about these recipients.

e) ***The right to restrict processing***

Individuals have a right to limit how NILGOSC uses data, including who the data is shared with. However, a request for information to be used for limited purposes will not delete the information NILGOSC holds. NILGOSC publishes a Privacy Notice, which outlines how it uses data and who it is shared with.

f) ***The right to data portability***

This right enables individuals to obtain copies of the information NILGOSC holds in a format that is easily transferred to either individuals or another organisation.

This is particularly relevant to members who may choose to transfer out of the Scheme to another pension provider. NILGOSC will provide the information it holds to a new pension provider in a format that they can use. A transfer out of the Scheme will only happen at the request of a member.

g) ***The right to object***

Individuals also have the right to object to the use of data for certain actions. NILGOSC may share information with third parties, which is detailed in its Privacy Notices. Should an individual exercise their right to object, it will not limit the information they receive from NILGOSC as it may be required by law to provide certain information. In such cases, NILGOSC will assess the request and take appropriate steps to comply with the request, where possible. However, NILGOSC must ensure that it also fulfils any legal obligation to provide information or supply services.

h) ***Children's data***

The GDPR ensures the protection of children's data as children may be less aware of the risks and consequences associated with the processing of their personal data. Compliance with the data protection principles and 'fairness' in particular should be central to any of NILGOSC's processing of children's personal data.

Any information held by NILGOSC which relates to the personal data of a child under 13 is held with the consent of a parent or guardian with parental responsibility. Children aged 13-16 are generally regarded as having the appropriate level of understanding to provide their own consent for the use of their data.

12. Exercising Your Rights

12.1 Where an individual data subject has a question or complaint regarding how their rights under GDPR are upheld, they are encouraged to make contact in writing or by email to NILGOSC's Data Protection Officer in the first instance.

12.2 Data subjects may exercise their right to access their personal data processed by NILGOSC by submitting a request to view or receive copies of their data. NILGOSC will endeavour to comply with such requests within one month, or in the case of complex requests, this timeframe may be extended for up to two months.

12.3 In exercising any of the other rights set out at section 11 above, such requests can be made verbally, in writing or by email. A response will be issued in writing or by email indicating whether or not NILGOSC can comply with the request and if so, the action to be taken. In the event that NILGOSC disagrees (e.g. the data is held for a legal purpose), the data subject may request their objection be recorded with the relevant record. NILGOSC will aim to comply with such requests with undue delay and, at the latest, within one month of receipt. The response will explain whether or not NILGOSC intends to comply with the request, including any parts of the request which NILGOSC considers impracticable or unjustified.

12.4 Data subjects may ask NILGOSC for an explanation of any decision likely to significantly affect them which has been, or may be, taken solely by wholly automated means. This will apply most specifically in the electronic calculation of pension benefits using NILGOSC's software management system. NILGOSC will consider such a request and consider reviewing a decision which has been taken, or consider taking a new decision on a different basis, in circumstances where either course of action is appropriate and timely, unless the automated decision qualifies as an exempt decision.

12.5 If a data subject remains dissatisfied with a response received, they may ask for the matter to be dealt with under NILGOSC's Complaints Policy.

12.6 Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the ICO to carry out an assessment of their case and/or pursue a legal remedy.

13. Key Personal Data Risks

13.1 The effective management of personal data is not simply about ensuring compliance with data protection legislation, but about following best practice guidelines for information security, information risk management and openness, accountability and transparency.

13.2 Personal data is a particularly sensitive type of information held by NILGOSC, and is factored into our information risk management processes. The key potential risks which this policy is designed to address are:

- Breach of confidentiality (information being disclosed inappropriately)
- Breach of security (unauthorised access to information)
- Failure to produce privacy notices or to gain positive consent when required
- Failure to establish efficient systems of managing change, leading to personal data not being up to date
- Insufficient clarity to staff and the public about the way data is used
- NILGOSC's service provider(s) failing to comply with the requirements set out in data protection agreements

13.3 NILGOSC assesses information risks in line with the Risk Management Policy, and information risks are recorded in the corporate risk register.

14. Roles and Responsibilities

14.1 All staff have a responsibility to manage personal data held by NILGOSC appropriately, in accordance with the Data Protection Policy and Data Protection Procedures. In addition, the roles listed below have specific information management responsibilities.

a) ***Senior Management Team:*** Overall responsibility for ensuring that NILGOSC complies with legal obligations, with this policy and with the Data Protection Procedures.

b) ***Senior Information Risk Owner (SIRO):*** This role is currently fulfilled by the Deputy Secretary, whose responsibilities include.

- Designated Data Controller for NILGOSC
- Owner of the Information Risk Assessment and the Information Risk Policy
- Provision of written advice to the Accounting Officer on the content of the annual Governance Statement in regard to information risk
- Oversight of appropriate controls to manage and mitigate personal data risks, including training for staff, managers and Committee Members.
- Ensuring that NILGOSC information management policies are maintained.

c) ***Data Protection Officer (DPO):*** This role is currently fulfilled by the Governance Manager (in their absence Head of Governance & Support Services), whose responsibilities include:

- Maintaining, reviewing and monitoring compliance with NILGOSC's information management policies.
- Monitoring and reviewing NILGOSC's processing activities to ensure they are consistent with the principles and individual rights under data protection legislation.
- Liaising with contract owners to ensure that appropriate data protection agreements are put in place with data processors and controllers.
- Briefing the SIRO on data protection responsibilities
- Handling Subject Access Requests and Freedom of Information requests
- ICO notification, including the reporting of personal data breaches
- Expert knowledge of data protection law and practices and the ability to fulfil the role and duties in line with Section 4, Article 39 of the GDPR.
- Providing advice when requested as regards to Data Protection Privacy Impact Assessments and monitor its performance as per Article 35 of the GDPR
- Ensuring that data protection induction and GDPR awareness training take place. More in depth training will be provided if staff are involved in personal data and special categories of personal data.
- Conducting a biennial review of information risk and the effectiveness of the information risk policy
- Approval of contracts with Data Processors.

d) ***Information Security Officer (ISO):*** This role is undertaken by the IT Systems Manager, who has the following responsibilities:

- Day to day responsibility for all aspects of information security
- Making decisions on information security matters
- Implementation and review of the Information Security Policy

- Information security incident reporting and resolution
- Provision of staff training on information security.

e) ***Information Asset Owners (IAOs):*** All teams in NILGOSC handle personal data. The IAO role is undertaken by Senior Managers responsible for each team in respect of the information assets and systems under their control. The role has the following responsibilities:

- Knowing what information is held, who has access and for what purpose.
- Ensuring that good data protection practice is followed by ensuring that staff adhere to the guidance set out in this policy and the Data Protection Procedures
- Understanding, identifying and responding to risks to information assets and systems
- Identifying and keeping a record of staff and contractors with access to, or involved in handling, individual records containing personal data
- Approving arrangements for the transfer of data, e.g. on removable media
- Approving information disposal mechanisms.

g) ***All NILGOSC staff are*** responsible for:

- Following policies and procedures for managing personal data
- Advising the Data Protection Officer or SIRO when they believe that the GDPR and DPA when enacted and/or this policy may have been breached
- Forwarding any Subject Access Requests to the Data Protection Officer and Corporate Support Officer for processing
- Ensuring that any information they provide to NILGOSC in connection with their employment is accurate and up to date.

The Data Protection Procedures provide further details on generic staff responsibilities for data protection.

- These responsibilities apply equally to full-time and part-time staff, temporary and agency staff, contractors and consultants.
- Breaches of this policy may result in disciplinary action.

15. Breaches of Policy

15.1 Breaches of this policy and/or security incidents can be defined as events which could have, or resulted in, loss or damage to an individual's personal data which is in breach of NILGOSC's security procedures and policies and data protection legislation.

15.2 It is mandatory to report high risk/materially significant breaches to the ICO within 72 hours of becoming aware of the incident. In some cases, the individuals affected will need advised within this period. The severity of the risk to individuals will be assessed in line with NILGOSC's Breach Reporting Procedure.

15.3 All employees, Committee members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through NILGOSC's Breach Reporting Procedure. This obligation also extends to any external organisation contracted to support or access NILGOSC's information systems.

15.4 In the case of third party vendors, consultants or contractor's non-compliance could result in the immediate removal of access to the system. If damage or compromise

of NILGOSC's ICT systems or network results from the non-compliance, NILGOSC may consider legal action against the third party.

15.5 Any incidents of a data breach or near miss should be reported to the Data Protection Officer, immediately and without undue delay.

16. Staff Awareness and Training

16.1 All staff must successfully complete an e-learning course in respect of data protection and must pass the associated test within four weeks of joining NILGOSC. Staff are also required to attend a mandatory training session on data protection and information security as part of their induction process.

16.2 All staff must undertake mandatory annual data protection refresher training.

17. Accountability & Compliance Monitoring

17.1 In order to demonstrate compliance with relevant data protection legislation and processing principles, NILGOSC will continue to:

- Have a designated Data Protection Officer, with appropriate knowledge and training.
- Implement appropriate technical and organisational measures, including regular review and update of the Policy and Data Protection Procedures and other related policies, staff training, internal audits of processing activities, review and testing of IT systems.
- Maintain relevant documentation on processing activities and update Privacy Notices, where appropriate.
- Implement measures that meet the principles of data protection by design and default, including data minimisation, transparency, improving security features on an ongoing basis.
- Use data protection impact assessments, where appropriate.

18. Review

18.1 The DPO will oversee the operation of this policy on behalf of the Senior Management Team.

18.2 The Data Protection Policy and Data Protection Procedures will be reviewed every three years, but may be reviewed more regularly to reflect any changes to relevant legislation.

18.3 NILGOSC will review and update this policy to ensure it remains consistent with the law, Codes of Practice issued by the ICO and relevant best practice guidance.

Published:	March 2010
Updated:	November 2011
Updated:	January 2013
Updated:	June 2015
Last Updated:	April 2018
Next Review Due:	April 2019

Appendix A

Article 6

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

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 part, 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.

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 L 119/36 EN Official Journal of the European Union 4.5.2016 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.

Appendix B

Article 9

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: 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. (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.