APPENDIX A

West Suffolk Councils'

Data Protection Policy

1. Executive Summary

1.1. This joint policy outlines the principles of the **General Data Protection Regulations 2018 (GDPR)** and identifies how both St Edmundsbury Borough Council and Forest Heath District Council (jointly referred to as West Suffolk councils throughout this policy) comply with the GDPR. It aims to give guidance on how the requirements of the GDPR apply to the work of the West Suffolk councils.

1.2. This policy covers all personal data that West Suffolk councils hold in either electronic or paper format, and applies throughout the life cycle of the data from the time it is created or arrives within the West Suffolk councils, to the time it is either destroyed or permanently preserved.

1.3. This policy applies equally to all West Suffolk councils' employees, agency staff, contractors and councillors.

1.4. This policy also:

1.4.1. Identifies responsibilities for data protection; and
1.4.2. Gives more specific guidance on the following areas:

1.4.2.1. Notification to the Information Commissioner
1.4.2.2. Special Categories of Data (sensitive personal data)
1.4.2.3. Staff records and monitoring
1.4.2.4. Use of CCTV
1.4.2.5. Retention and disposal of personal data
1.4.2.6. Data subject access requests
1.4.2.7. Disclosure of data to third parties.
1.4.2.8. Privacy notices
1.4.2.9. Data breach
1.4.2.10. Training and awareness
1.4.2.11. Security

1.5. Further guidance is available on the Information Commissioner's website at the following link: Information Commissioner's Office

2. Context

2.1. GDPR balances the legitimate needs of organisations to store and use personal data with the rights of individuals who are the subject of this data. Basically, if an organisation collects or holds information about an identifiable natural person, or if it uses, discloses, retains or destroys that information, it is likely to be processing personal data.

2.2. GDPR is underpinned by a set of six straightforward, common sense principles which, if followed, will ensure

compliance with GDPR. GDPR also requires that 'the controller shall be responsible for, and be able to demonstrate compliance with the principles' – this is referred to as accountability. These principles are set out at 3.2 below.

2.3. Compliance with GDPR is monitored and enforced by the Information Commissioner's Office (ICO). The ICO has the power to impose sanctions, including fines of up to £17 million for a serious breach of one or more of the principles and where the breach is likely to cause substantial damage or distress. The ICO can also impose additional fines of up to £8.5 million for breaches of an organisation's governance procedure (accountability). This is in addition to any penalties imposed by the courts against individuals who unlawfully breach GDPR or violate Article 8 of the Human Rights Act – The Right to Privacy.

2.4. GDPR uses many terms which have a specific meaning in the context of these regulations, and therefore a glossary of these terms is included at the end of this policy.

2.5. West Suffolk councils collect and use certain types of data about people, in order to continue to provide the level of service expected by the public and to comply with the requirements of government departments. This data includes personal details about current, past and prospective staff, suppliers, West Suffolk taxpayers, benefits claimants, social housing and other tenants, residents in West Suffolk and others with whom they communicate.

2.6. As organisations which deal with personal data the West Suffolk councils will ensure they:

2.6.1. Comply with both the law and best practice

2.6.2. Respect the rights of individuals

2.6.3. Are open and honest with individuals whose data is held

2.6.4. Provide support and training for those who handle personal data, so that they can act confidentially and consistently.

3. Achieving Compliance with the General Data Protection Regulations – Principles

3.1. The main purpose of the six principles of GDPR is to protect the interests of individuals whose personal data is being processed (i.e. information or data obtained, recorded or held, or the carrying out of any operation or set of operations on the information or data). They apply to everything West Suffolk councils do with personal data, except where an exemption applies. The key to complying with GDPR is to follow the six principles relating to the processing of personal data.

3.2. Below is a summary of the six principles and the ways in which West Suffolk councils comply with them.

3.3. This first principle states that personal data shall be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**) and in particular, shall not be processed unless:

3.3.1. At least one of the conditions in Article 6 of GDPR is met; and

3.3.2. In the case of special categories of personal data (sensitive), at least one of the conditions in Article 9 of GDPR is also met.

3.4. In practice, this means that West Suffolk councils must:

3.4.1. Have legitimate grounds for collecting and using the personal data

3.4.2. Not use the data in ways that have unjustified adverse effects on the individuals concerned

3.4.3. Be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data

3.4.4. Handle people's personal data only in ways they would reasonably expect

3.4.5. Make sure they do not do anything unlawful with the data

3.5. We do this by:

3.5.1. Abiding by the law in all activities

3.5.2. Ensuring data subjects are aware of how their data will be used at the time they provide it and not using it for any purpose incompatible with the original stated purpose

3.5.3. Ensuring the data has been provided by a person who is legally authorised, or require, to provide it

3.5.4. Ensuring that the processing of personal data meets one of the legitimising conditions listed in Article 9 of GDPR

3.5.5. Ensuring that all processing of personal data meets one of the following conditions:

3.5.5.1. The date subject gives consent for one or more specific purposes

3.5.5.2. The processing is necessary to meet contractual obligations

entered into by the data subject

3.5.5.3. The processing is necessary to comply with the legal obligations of the controller

3.5.5.4. The processing is necessary to meet the vital interests of the data subject

3.5.5.5. The processing is necessary for tasks in the public interest or exercise of authority vested in the controller

3.5.5.6. The purposes of legitimate interests pursued by the controller

3.6. Further conditions are in place for special categories of personal data, see section 6 for further guidance

3.7. The second principle states that personal data shall be 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 purpose (**purpose of processing**)

3.8. In practice this means that we must:

3.8.1. Be clear ('explicit') from the outset about why they are collecting personal data and what they intend to do with it

3.8.2. Comply with Article 13 of GDPR requirements – including the duty to provide privacy notices to individuals at the point of collecting their personal data

3.8.3. Ensure that if West Suffolk councils wish to use or disclose the personal data for any purpose that is additional to or different from the original specified purpose, the new use is compatible with the original specified purpose

3.9. We do this by:

3.9.1. At the time data is obtained the data subject will be informed of the purpose for which the data is being collected. Purposes may be specified in a privacy notice given in accordance with Article 13 requirements

3.10. The third principle states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed (**data minimisation**)

3.11. In practice this means:

3.11.1. Data must be the minimum necessary for fulfilling the purpose for which they are processing them

3.11.2. They do not collect information they do not need

3.11.3. The data must be adequate for need

3.12. We do this by:

3.12.1. Collecting only the minimum amount of personal data required to fulfil the processing needs, or to comply with legal requirements. Additional unnecessary data will not ber collected and data will not be held on the off chance that it might be useful in the future

3.13. This fourth principle states that personal data must be accurate and where necessary, kept up to date (**accuracy**)

3.14. We do this by:

3.14.1. Taking reasonable steps to ensure the accuracy of any personal data obtained; ensure that the source of any personal data is clear; carefully consider any challenges to the accuracy of the information; consider whether it is necessary to update the information

3.15. This fifth principle states that personal data should be kept in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed (**retention**)

3.16. In practice this means we will need to:

3.16.1. Review the length of time we may lawfully keep personal data

3.16.2. Consider the legitimacy of purpose or purposes for which the council hold information in deciding whether (and for how long) to retain it

3.16.3. Securely delete information that they are not holding lawfully or legitimately

3.16.4. Update, archive or securely delete information if it goes out of date

3.17. We will do this by:

3.17.1. Only holding personal data as long as it I is necessary for the lawful processing purpose for which it has been provided/obtained

3.17.2. If personal data is collected for a specific project it shall be disposed of as soon as the project comes to an end

3.17.3. Complying with our record retention guidance (available on the West Suffolk website)

3.18. The last principle states that personal data should be processed in a manner that ensures appropriate security of the

personal data (**security**)

3.19. In practice this means we will need to:

3.19.1. Ensure a level of security appropriate to the nature of the data and harm that might result from a breach of security

3.19.2. Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach

3.19.3. Be ready to respond to any security incident swiftly and effectively

3.19.4. Be sure there is the right physical and technical security, backed up by robust policies and procedures and reliable well trained staff

3.19.5. Be clear about who in the organisation is responsible for organising information security

3.20. We will do this by ensuring we have robust technical and organisational security measures including (amongst others):

3.20.1. Password protection of computer systems

3.20.2. Controlled access to West Suffolk council buildings

3.20.3. Access rights of users appropriate to the needs of their job

3.20.4. Management to ensure that performance with regard to personal data is regularly assessed and evaluated

3.20.5. All staff to have a level of understanding of GDPR commensurate with their duties

3.20.6. Adequate checks to ensure the suitability of all staff who have access to personal data

3.20.7. Management to ensure that everyone managing and handling data is subject to appropriate line management

3.21. West Suffolk councils shall have in place appropriate security arrangements covering both physical and technical safeguards. See section 15 for further details.

4. Record of Processing Activities

4.1. The councils maintain a record of processing activities capturing much of the above, capturing: a) the condition relied upon for the processing, b) how the processing satisfies Article 6 of GDPR and c) whether the personal data is retained and erased in accordance with the Document retention Guidance

5. Roles and Responsibilities

Data Controllers

5.1. For the purpose of GDPR the data controllers are Forest Heath District Council and St Edmundsbury Borough Council

Senior Information Risk Officer

5.2. West Suffolk's Senior Information Risk Officer (SIRO) with specific responsibility for managing information risks on behalf of the Chief Executive and members of West Suffolk will be one of the Councils' Directors as designated by the Chief Executive.

Information Governance Working Group

5.3. The Information Governance Working Group (IGWG), chaired by the SIRO, provides an oversight of the proper and secure handling of information by the West Suffolk and supports the SIRO in his role

Data Protection Officer

5.4. West Suffolk councils' Data Protection Officer with specific responsibility to ensure the West Suffolk councils are compliant with the DPA is the Councils' Monitoring Officer.

Data Protection Coordinator

5.5. The Data Protection Coordinator will act as a link officer between services and the Data Protection Officer when there is an issue relating to data protection

5.5.1. Advise the Data Protection Officer if a data subject access request has been received in any service area and support the service in drawing up its response (simple and complex)

5.5.2. Maintain a data / privacy breach notification procedure and register, and assist the Data Protection Officer in reviewing breaches, why they arose and potential system improvements which may be required

5.5.3. Review the various application forms used within services to ensure they include the reasons why West Suffolk councils need to collect and store the personal information requested, and how they will use this information (privacy notices)

5.5.4. Determine the extent to which personal information is shared with others and whom it is shared with (internally and externally)

5.5.5. Conduct a regular review of the types of personal data being processed by services, reporting any changes to the Data Protection Officer and ensuring compliance is maintained

5.5.6. Maintain a training and awareness programme

5.5.7. Support services in undertaking Data Protection Impact Assessments

Assistant Directors

5.6. Assistant Directors have responsibility for ensuring that their service area complies with the principles of GDPR when processing personal data. This includes ensuring that all staff are aware of their responsibilities under GDPR and trained to discharge those responsibilities

Staff

5.7. All staff have a responsibility to ensure that they comply fully with GDPR. It is a criminal offence to knowingly or recklessly obtain or disclose personal data. They should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under West Suffolk councils' disciplinary procedure.

Councillors (Members)

5.8. Councillors must comply with this policy when handling personal data on council business, and be aware of their responsibilities as individuals under GDPR. Although the Data Controller is liable for any mishandling of personal data, Councillors should be mindful that it can be a criminal offence for which they would be personally liable if they were to process personal data in a manner which they know that they are not authorised by the Data Controller to do. A breach of this policy by a Member is a potential breach of the Code of Conduct.

6. Notification

6.1. The ICO maintains a public register of data controllers. GDPR requires every data controller who is processing personal data to notify and review their notification, on an annual basis.

6.2. It is an offence under GDPR if the notification is not kept up-to date, and also an offence to use personal data in a manner which has not been notified.

6.3. It is the responsibility of all Assistant Directors to advise the data protection coordinator of any changes to the uses of personal data within their service areas as soon as they occur so that West Suffolk councils' notification can be updated

6.4. West Suffolk council's notification will be reviewed annually and kept up-to-date by the Data Protection Officer

6.5. A copy of West Suffolk council's current notification can be viewed at the Information Commissioner's website: www.ico.org.uk

7. Special Categories of Personal Data (Sensitive)

7.1. Extra care must be taken when processing special categories of personal data as additional requirements under GDPR must be met to ensure that the processing is legitimate and safe. At least one of the legitimising conditions described under Article 6, and also one of the legitimising conditions (Article 9) shown below, must be met.

7.2. 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.

7.3. Paragraph 7.2 shall not apply if one of the following applies

7.3.1. The data subject has given explicit consent
7.3.2. It is necessary to fulfil the obligations of controller and data subject
7.3.3. It is necessary to protect the vital interests of the data subject
7.3.4. Processing is carried out by a foundation or not for profit organisation
7.3.5. The personal data has been made public by the data subject
7.3.6. Establishment, exercise or defence of legal claims
7.3.7. Processing is necessary for reasons of substantial public interest
7.3.8. Processing is necessary for the purposes of preventative 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
7.3.9. Reasons of public interest in the area of public health
7.3.10. Archiving purposes in the public interest

7.4. The advice of the Data Protection Officer or their duly authorised deputy should be sought before the processing or collection of sensitive personal data for any new purpose commences.

8. Staff Records and the Monitoring of Staff

8.1. West Suffolk councils should comply with the ICO's *'Employment Practices Code'* in relation to the processing of staff personal data. This Code is intended to help employers comply with the DPA and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of staff that personal data about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own organisations carrying out their legitimate business.

8.2. In particular, staff monitoring should only be carried out in accordance with this Code. A copy of the Code is available on the ICO website at the following link: Employment Practices Code

9. CCTV Monitoring

9.1. CCTV monitoring must only be carried out in accordance with the ICO's *'CCTV Code of Practice'*. A copy of this Code is available on the ICO website at the following link: CCTV Code of Practice

10. Retention and Disposal of Personal Data

10.1. It is the responsibility of the service areas holding personal data to ensure that the data they hold is kept accurate and up-to-date, and is not held for any longer than is necessary for the purpose for which it was collected.

10.2. When the data is no longer required the service area must dispose of the data safely. Guidance on retention periods for classes of data is set out in the West Suffolk councils' record management guidance which is available on the West Suffolk website

11. Data Subject Access Requests (DSARs)

11.1. It is one of the fundamental rights of the individual under GDPR to be able to access their information. Individuals will have the right to obtain:

11.1.1. Confirmation that their data is being processed
11.1.2. Access to their personal data
11.1.3. Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

It is in the interests of the West Suffolk councils to have an open and honest approach with all individuals on which they hold data.

11.2. GDPR sets out guidance and a time limit within which a DSAR must be answered.

11.3. Any individual requesting access to their personal data is asked to complete a request in writing which must be referred to the Data Protection Officer. This gives clarity around the date the request was made and therefore the deadline date and also encourages the individual to think clearly about the data they require. Guidance regarding DSARs is available on West Suffolk councils' website at: How we use information which includes access to a DSAR application form which may be printed off and completed.

11.4. The individual making the request must produce a document such as a passport or driving licence to confirm his identity.

11.5. West Suffolk councils will approach all requests for data in an open and honest way and seek to ensure that the individual gets all the data they require as long as this is permissible within the law.

11.6. There will be some requests where it will not be possible or appropriate to release personal data, for example, when doing so would involve releasing personal data about another individual, or if the data relates to ongoing criminal investigations. Any concerns about releasing data should be discussed with the Data Protection Officer or their duly authorised deputy prior to release of the information.

11.7. More information on the procedure for recognising and responding to a DSAR can be found on the K:drive/Data Protection

12. The Right to be informed and Privacy Notices

12.1. The right to be informed encompasses the councils' obligation to provide fair processing information, typically through a privacy notice. It emphasises the need for transparency over how the councils' use personal data.

12.2. The information supplied in the privacy notice is determined by whether or not the personal data was obtained directly or indirectly from the individual.

12.3. The information the councils' supply about the processing of personal data must be:

12.3.1. Concise, transparent and easily accessible
12.3.2. Written in clear and plain language, particularly if addressed to a child
12.3.3. Free of charge

12.4. Further guidance on how to comply with 'the right to be informed' is provided in the: ICO privacy notice code of practice

13. Sharing Personal Data

13.1.1. Where requests are received from external organisations or third parties for personal data about individuals, advice should be sought from the Data Protection Officer or their duly authorised deputy unless there is an up-to-date information-sharing/data exchange agreement in place with that organisation or third party. **Under no circumstances** should any personal data about any individual be passed outside West Suffolk councils without the authority of the Data Protection Officer or their duly authorised deputy unless an approved data sharing agreement is in place. Where an officer considers information about a child or young person must be disclosed to a third party under the safeguarding provisions they must do so in accordance with West Suffolk councils'

Safeguarding Children and Young People Policy – a copy can be found by clicking the link: Safeguarding

13.2. Agencies which request data on a regular basis such as the police or banks will have easy access to appropriate paperwork and guidance for use in these circumstances.

13.3. It should be noted that whilst staff understandably will wish to assist external agencies wherever possible especially if the request relates to criminal activity (for example the police or banks), West Suffolk councils are under no obligation to release personal data unless the request is made by a court order.

13.4. Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasions it may be appropriate to publish personal data with the individual's consent. However, in such cases staff must ensure consent is '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'. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

13.5. Staff should be aware that publishing personal data on West Suffolk councils' web pages or on the internet by any other means effectively means that the data is published world-wide and outside the European Economic Area. This means it cannot be protected by GDPR or the European Directive on Personal Privacy. Great care should be taken before publishing any personal data (or any data from which individuals could be identified) in this manner and the approval of West Suffolk councils' Data Protection Officer and Senior Information Risk Owner or their deputies should be obtained before publication.

14. What to do in the Event of a Data Breach

14.1. The ICO defines a data breach as 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 in connection with the provisions of a public electronic communications service'.

14.2. A personal data breach includes but is not restricted to the following:

14.2.1. The accidental alteration or deletion of personal data

14.2.2. The transfer of personal data to those who are not entitled to receive it

14.2.3. Unauthorised access to personal data

14.2.4. Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could not have reasonably contemplated

14.2.5. Theft of storage devices

14.3. If a member of staff becomes aware of a data breach their first action should be to inform their line manager, who will then ensure that the breach is reported to the Data Protection Officer or their duly authorised deputy.

14.4. The Data Protection Officer or their duly authorised deputy will then decide on the most appropriate steps to take depending on the nature and quantity of data released. An investigation will be carried out into all data breaches.

14.5. The ICO will be informed of all serious data breaches where significant harm to an individual(s) is likely or a large number of individuals are affected.

15. Training and Awareness

15.1. In order to fully comply with GDPR it is important that all staff who have access to any personal data have an awareness of the regulations.

15.2. Training is a crucial element of staff awareness. West Suffolk councils' staff must be aware of their obligations relating to personal data as part their duties.

15.3. Training may be achieved in a number of ways:

15.3.1. all staff to be made aware of this Data Protection Policy;

15.3.2. e- learning tools; and

15.3.3. in-house training provided by the Data Protection Officer or their duly authorised deputy.

15.4. For some posts additional training and guidance is required. Those posts will identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

16. Keeping Information Secure

16.1. The Sixth Principle of GDPR requires organisations to take appropriate technical and organisational measures to keep data secure. The security of data held by West Suffolk councils is a relatively complex area and more information on the technical

details of information security can be found in the West Suffolk Information Security Policy: Information Security Policy

16.2. However, security of data goes beyond the use of computer equipment. Data will inevitably be stored or processed in hard copy forms at some time and access to this must be restricted to only those authorised to view it. As a general guide hard paper copies should not be left in the open in offices but should be kept locked away when not in use, in the same way as computer terminals should not be left unlocked and unattended.

16.3. It is important to remember that individuals should only be able to access data which they need to do their job. Personal data should not be left unattended and freely available to anyone in the office.

Working from home

16.4. When working from home, officers must ensure they only use their encrypted laptops to access personal data electronically. Paper files which include personal information must be kept in secure cases (lockable) at all times when not in use.

16.5. UNDER NO CIRCUMSTANCES should hard copy files be left unattended.

17. Administration

17.1. The Data Protection Officer has overall responsibility for the maintenance and operation of this policy, and will be pleased to answer any questions about it.

17.2. Responsibility for monitoring adherence to this policy belongs with the Information Governance Working Group.

17.3. This policy will be reviewed at least every two years to confirm it reflects best practice and to ensure it complies with any legislative changes or amendments. Any significant and necessary changes will be made by the Senior Information Risk Officer and the Data Protection Officer.

GDPR Glossary of Terms

For the purposes of this Regulation:

1. '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;

2. ‘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;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

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

6. ‘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;

7. ‘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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. ‘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;

10. ‘third party’ means a natural or legal person, public authority, agency or body 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;

11. ‘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;

12. ‘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;

13. ‘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 from the natural person in question;

14. ‘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;

15. ‘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;

16. ‘main establishment’ means:

    16.1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

    16.2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

    22.1. the controller or processor is established on the territory of the Member State of that supervisory authority;

    22.2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

    22.3. a complaint has been lodged with that supervisory authority;

23. ‘cross-border processing’ means either:

    23.1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

    23.2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

26. ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.