Department for Culture Media & Sport –
Calls for views on the General Data Protection Derogations
10 May 2017

Response from: AXA UK Plc, a UK General Insurance Company has around 11 million customers in the UK and operates through specific operating companies – AXA Insurance and AXA PPP healthcare.

To: Data Protection Team
Department for Culture, Media & Sport

AXA UK takes its responsibility to protect and safeguard personal data very seriously. AXA UK also considers its obligations to provide Insurance, including insurance which includes health related cover as a critical service for current and future customers. For this reason we have responded to the Calls for views. Our response is in order of priority for the Department for Culture Media and Sport (DCMS) to consider necessary derogations to ensure the continuance of this important service across the UK when implementing Data Protection law into the UK.

Theme 5 – Archiving and Research

The derogations related to archiving and research includes article:

Article 89 – Safeguards and derogations relating to the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Response: Article 89;

Derogation is required in respect of Article 89 (2). Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law for the rights referred to in;

Article 15; - Right of access by the data subject (Recitals 63, 64);
Article 16 - Right to rectification (Recital 65);
Article 18 - Right to restriction of processing (Recital 67; and
Article 21 - Right to object (Recital 69, 70) subject to the conditions and safeguards referred to in paragraph 1 (Article 89);

Whereas; "*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject*".

The General Data Protection Regulation (GDPR) allows for principles that may include pseudonymisation and minimisation provided that those purposes can be fulfilled in a manner that does not render impossible or seriously impair the achievement of the

specific purposes, and as such derogations are necessary for the fulfilment of those purposes.

Therefore, in order for insurers to continue to process personal data for statistical purposes under the GDPR, derogations are required to restrict obligations and rights in respect of:

Article 21: Right to object

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

AXA UK has consistently communicated to the Information Commissioner's Office (ICO) and DCMS both through the Association of British Insurers (ABI) and directly underlining the principles of Insurance Underwriting Practices. This includes the life-cycle of this processing and the need for detailed analysis to achieve an ultimate and optimum outcome for customers. The majority of this analysis takes place by qualified actuarial, pricing and claims personnel supported by technology. The outcomes are defined by rate setting, scheme performance, cost analysis, trend analytics, supplier monitoring and fraudulent behaviours.

Article 89 allows Member States to provide for Analytics for Statistical purposes including the ability to consider necessary safeguards to maintain the rights and freedoms of the data subject. Furthermore, Article 89 makes possible statistical analysis without constraints imposed by Article 15, Article 16, Article 18 and Article 21. We would further suggest Member States extend the flexibility of this Article to include Article 17 and Article 20 and for the UK Government to consider Underwriting practices by exception where personal and sensitive personal data is included, permitted to the extent if disallowed, the required outcome would be rendered impossible or seriously impaired.

The lawfulness of processing, data processed for statistical purposes is based on Article 6(1) (b) performance of a contract, or (f) necessary for the purposes of the legitimate interests pursued by the controller. Without a specific derogation data subjects may object to processing for statistical purposes. Underwriting practices require personal data to achieve the optimum price to cover the risk based on the factors provided by the data subject.

A better understanding of the customer through data is evidenced through competitive premiums. The same applies to analysis of claims data which may include health data. Article 9 does not currently permit Health data to be processed for the performance of a contract. This constraint is addressed under Theme 7, Sensitive personal data and exceptions. The same principles apply to Sensitive data as set out above in respect of Article 89 for insurers to continue to process sensitive data for statistical purposes.

Theme 7 – Sensitive personal data and exceptions

Sensitive personal data and exceptions The derogation related to Sensitive Personal Data and Exceptions include articles: Article 9 – Processing of special categories of personal data.

Response: Article 9 Health Data (see below for Article 9 Employee Data)

Without explicit consent Underwriting, which includes special category personal data, such as Health data cannot be processed.

Additionally, if Underwriting is considered as Profiling as set out in Article 22 and consent provided for health data is withdrawn it would not be possible to continue to provide the insurance contract which included special category personal data, rendering contractual liabilities unclear.

Article 9(g) provides the opportunity for the UK Government to intervene where the provision of insurance (Underwriting) is considered to be in the public interest, and where Member State law has the opportunity to provide for specific measures in the interests of the data subject. We consider it is in the interests of the public to ensure Underwriting practices are maintained to provide readily available accessible insurance products.

Current UK legislation has been implemented for the very purpose of processing health data, and data on behalf of beneficiaries for this purpose;

> Statutory Instrument 2000 No. 417 (The Data Protection (Processing of Sensitive Personal Data) Order 2000) which allow insurers to process fraud, process certain health data without explicit consent (enabled through Recital 10 or Article 9 (4) and further the recognition of principles in the Consumer Insurance (Disclosure and Representations) Act 2012, which allows an individual to act on behalf of, or as agent, and provide information on behalf of another in order to obtain insurance cover.

The ICO Consent Consultation notes "that explicit consent is one way to legitimise processing special category personal data, with some scope for UK legislation to add more". Without an exception for 'Sensitive data as part of an Insurance Contract' as is now, the process of providing an insurance contract, whether for Health or Travel (pre-existing health, or dealing with motor accidents) would be complex and disruptive for the policyholder.

These disruptions would occur at claims stage at a time when the individual may be in peril, (i.e. an accident abroad or a car accident). We believe the additional requirement to obtain a necessary consent before the claim can be processed would not be the individual's principle focus or in their interests. In addition, the requirement for onward transfer of health data to organisations remains essential in the provision and administration of insurance, obtaining consent in advance of this process would be disproportionate and unviable.

Without a specific derogation to process Health data without consent when sensitive data is included means there is no legal basis within GDPR to respond to an individual's claim, especially if the individual is not in a position to a) provide consent and where b) Article 9(c) is not appropriate. Currently SI 417 currently provides the legal basis for processing sensitive data for insurance business.

Furthermore, Recital 43 states "*Consent is presumed not to be freely given… if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*." The process of entering into an Insurance Contract is determined by the provision of information, and in some cases sensitive information. Therefore it would not be possible to objectively comply with the requirements of Article 7(4) and Recital 43 as explicit consent to process sensitive data is required when health data forms part of the contract, making this a conditional consent.

It was proposed in the ICO Consent Consultation that the insurance company is required to provide names and details of all third parties who will be relying on consent (which would relate to Health Data under Explicit Consent, i.e. Travel/Health Insurance). These parties would vary from policy to policy dependant on the available agent, location, commercial arrangement, and type of service. It is highly possible that the dependence on explicit consent for processing insurance would negatively impact the process to the detriment of the data subject, most likely at claims stage, when the customer is at their most vulnerable. Similarly, the reliance on consent for processing at claims stage for a travel claim is likely to be problematic when dealing with a local country agent in another language and similar complexities.

There are other circumstances which are unique to the insurance sector where Health data is passed on for insurance related purposes. For example an insurance company may re-insure the risk out to a reinsurance organisation to manage the maximum exposure the primary insurer and could include any one claim or set of claims within a portfolio. This is a commercial practice to reduce the expense for the primary insurance company. The risk transferred may or may not include health related data. At the point of purchase, the insurance company would not necessarily have made the commercial decision to reinsure to share risk where appropriate. The process is determined by the Insurance Treaty arrangements which could be based on a) the 12 month period value or b) individual high value claims. This is common practice, but without explicit consent from the policyholder risk sharing of this nature would prohibited. This is a practice which shares the risk across specialists within the UK Insurance Sector. The nature of Reinsurance practices within the UK Insurance market

should be explored in detail by the UK Government as this is a common commercial practice within the UK Insurance Sector.

In addition to the existing Statutory Instrument No. 417, and as noted above, it is also necessary to maintain the Consumer Insurance (D&R) Act 2012 which authorises one party to act on behalf of another. Without this, family Travel Policies, named Drivers for Motor Vehicle and Company Health Schemes will be rendered unviable in their current form, again removing existing cover from current and future policyholders.

Examples:

A family member is organising ski insurance for a family trip for all parties departing the following day; his young adult child (aged 18) is not with the main policyholder at the time, but meeting him before they depart. The child has asthma and so the main policyholder would not be able to discuss this with the insurance company directly without his son's consent. A second call may not be possible due to the departure date, obtaining any further information for that family travel policy may not therefore be completed, or elements not covered.

'Customer First' forms the cornerstone of AXA's culture. First-hand experience tells us that a the majority of home, travel, motor and health policies organised for family members are done so by a family member responsible for the well-being of that family; the same would also apply for organisations providing insurance for their employees and families. It is likely there will be a deluge of dis-satisfied customers as they would not be permitted to organise cover for those they are responsible for and are dependent on a secondary call with another family member seeking consent, if sensitive data forms part of that policy. This will also be problematic where nominated spokespersons (i.e. interpreters, adult children acting on behalf of elderly parents) are prohibited from seeking quotes, or purchasing insurance on behalf of an individual for which they have taken responsibility.

In some cases when an individual books a travel policy the insurance company will ask "*if there is any known circumstances relating to close family members which could a) cause the policyholder to cancel departure or b) require the policyholder to return home*". If the policyholder does not disclose this information, and subsequently has to return to the UK as a direct result of a close family member's health, the return trip would not be covered as the policyholder had not disclosed this information about another close family member.

A similar position may arise relating to Motor Insurance. The question is asked, "*whether there are any restrictions relating to other named drivers*", the main policyholder would not be able to provide this information on behalf of a named driver. For example; a father calls to add his son to the policy, the son has a medical condition, but the father cannot discuss this on the son's behalf. A second call or subsequent follow-up with the insurance company and the son would then be required. The son may not contact the insurance company and, in the event there was an accident which was a direct result of the son's illness the son and any other party involved would not be insured.

Article 22 relates to underwriting practices where data is analysed through mathematical decision making algorithms to determine the technical price, i.e. the premium to cover the risk. The benefit of this practice has been noted in the recent ICO Big Data paper[1]. For non-sensitive data, an individual can object to Article 22 processing whereby the Data Controller would further explain how this is a legitimate process to establish optimum pricing, forming a contract. However, if an individual withdraws consent for processing sensitive data which forms part of a Health, Travel, or Motor policy, it would not be possible to continue to provide the contract to the data subject/policy holder, rendering contractual liabilities unclear.

The above provides details of the complexities of current Underwriting practices specific to the processing of sensitive data as part of an insurance contract when introducing explicit consent as required under the GDPR. Maintaining both the existing SI 417 and the Consumer Insurance (D&R) Act 2012 addresses these complexities where Health data forms part of the insurance contract and where the main policyholder acts on behalf of others.

The DCMS has the opportunity to provide the necessary derogation for processing sensitive Data, and where the main policyholder acts on behalf of another. We consider this should also be provided for when sensitive data, such as Health data forms part of an Insurance Contract.

A Derogation is required to allow insurers to continue to be able to process special categories of personal data as part of carrying on insurance business without explicit consent, this is particularly applicable to data concerning the health of the data subject, and where one party acts on behalf of another. AXA UK supports the UK Insurance Industry's proposal to resolve the issue of explicit consent through the insurance chain, with a as a specific and new legal basis under Article 9 where "*the processing is necessary for the arranging, underwriting and administration of insurance and reinsurance policies and insurance and reinsurance policy claims*". This specific derogation would also address the need for a separate derogation for Article 10.

Response: Article 9 Employee Data

Article 9(2)(b) allows Member States to provide a Derogation for processing sensitive personal data in the field of employment. The majority of employees are subject to employment contracts and currently within employment contract the requirement is set out to process personal and sensitive information for the purpose of employment, which the employee signs to agree. To maintain this provision and to ensure UK legalisation aligns with Recital 43 would require a derogation to process sensitive personal data in the field of employment and would be a necessary from the UK Government in the implementation of GDPR into UK law.

[1] FCA mandates ensure Insurance companies provide for all policyholders, including vulnerable individuals.

Theme 8 – Criminal Convictions

Criminal Convictions The derogation related to criminal convictions including articles: Article 10 – Processing of personal data relating to criminal convictions and offences.

Response: Article 10

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

Current legislation allows insurers to identify fraudulent activity and to cross-reference information with other fraud databases. This benefits honest customers, insurers and wider society by detecting crime and reducing premiums by lowering the levels of fraudulent claims. The requirement to maintain this provision will allow the use of conviction and offence data to identify risk, underwrite, price accurately, handle claims and help to detect and prevent fraud.

In order for an insurer to price risk correctly, it draws on as much information as possible to make an accurate risk based decision. If the insurer is prevented from using other data sources to understand fraud risk standardised pricing will have to be used which will inevitably mean that people pay more to cover the overall cost of claims.

Having a clear understanding of a driver's propensity to drive at speed (determined by points) allows the underwriter to determine the appropriate level of risk. If a UK exemption is not introduced, then insurers will not be able to use criminal convictions and offences data to identify risk, underwrite, price accurately, handle claims and to help detect and prevent fraud as is currently possible.

In addition to this, it is important that we interact with fraud related bodies such as the Insurance Fraud Bureau to perform due diligence on our customers. A failure to make appropriate provisions for the possibility that fraud is occurring at point of quote, point of sale and post-sale underwriting stages only leads to a poorer customer experience at claims stage and the possibility of innocent customers paying an increased premium to allow for a shortfall in an individual insurer's fraud controls. The processing of such data by insurers also helps act as a disincentive for criminal behaviour, and contribute to a safer environment and society with less of a burden on public service resources.

The most effective information provides for the most effective price. If the insurance industry is unable to analyse fraud data ultimately premiums will increase to address heightened claims costs.

Data is also processed in order to counter Financial Crime and positive matches are referred directly to the National Crime Agency ensuring potential serious and organised crime can be investigated by the appropriate agency as a further means to protect the public.

A Derogation is required by the UK to allow insurers to continue to be able to process data relating to criminal convictions and offences as part of carrying on insurance business, price accordingly and deter criminal behaviour.

Theme 9 – Rights and Remedies

The derogations related to Rights and Remedies include Articles:

Article 17 – Right to erasure ('right to be forgotten')
Article 22 – Automated individual decision-making, including profiling
Article 26 – Joint Controllers
Article 80 – Representation of Data Subjects.

Article 17 – Right to erasure. Current UK legalisation requires Insurance Companies to maintain records for a period of time, generally under the Statute of Limitations. This is to satisfy contractual obligations, or potential legal claims. The right to erasure would apply following the legal retention period, at which time the Insurance Company will delete records which are no-longer bound by UK legal requirements. The same responsibility applies to the Data Controller under Article 18(1)(c), Article 18(2).

Article 22 –Automated individual decision making, including profiling

Insurers need to be able to underwrite risks individually and such underwriting requires analysis and validation of data to achieve the best outcome for the individual. The greater the understanding of the individual the better the service of existing and the provision of future products is likely to be. Underwriting is the use of data analysed through mathematical decision making algorithms to determine the technical price, i.e. the premium to cover the risk. We consider underwriting to be a unique, highly regulated practice to the benefit of the wider public and not as defined under Article 4(4) of the GDPR.

For non-sensitive data, an individual can object to Article 22 processing whereby the Data Controller would further explain how this is a legitimate process to establish optimum pricing, forming a contract. However, if an individual withdraws consent for processing sensitive data which forms part of a Health, Travel, or Motor policy, it would not be possible to continue to provide the contract to the data subject/policy holder creating legal uncertainty.

Therefore a derogation under Article 22 for Underwriting practices, where insurance forms part of a contract should be considered by the DCMS, with particular reference to the application of Article 22(3) and Article 22(4).

Article 26 – Joint Controllers – The ability to determine the lead Data Controller by the Member State derogations should be upheld in the UK.

Article 80 – Representation of Data Subjects – The ability to determine a non-for-profit body to represent the data subject Derogation should be upheld in the UK, to the extent this is not a private body and under the scrutiny of the UK Government or Data Protection Supervisor.

Theme 13 – Restrictions

Article 23 permits Member States to legislate domestically measures which restrict the application of various rights and duties under the Regulation. The restrictions may apply to all of the individual rights in articles 12-22, and to the data protection principles in Article 5 in so far as they correspond to the Article 12-22 rights. The scope of Article 23 effectively continues similar restrictions that exist under the Current Directive and which were used in the Data Protection Act (DPA) to shape appropriate exemptions from the requirements of the DPA where that was permissible.

The derogations related to restrictions include Articles:

Article 23 – Restrictions.

1. *Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*

   (a) national security;
   (b) defence;
   (c) public security;
   (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
   (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
   (f) the protection of judicial independence and judicial proceedings;
   (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
   (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g)
   (i) the protection of the data subject or the rights and freedoms of others;
   (j) the enforcement of civil law claims.

2. *In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:*

   (a) the purposes of the processing or categories of processing;
   (b) the categories of personal data;
   (c) the scope of the restrictions introduced;
   (d) the safeguards to prevent abuse or unlawful access or transfer;
   (e) the specification of the controller or categories of controllers;
   (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;(g) the risks to the rights and freedoms of data subjects; and
   (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

The ability to (Article 23(1)(d)) maintain the prevention, instigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; must be upheld in the UK.

The ability to (Article 23(1)(e)) achieve other important objectives where they are important to economic or financial interests of the Union or of a Member State including monetary, budgetary and taxation matters, public health and social security; where this is necessary for reasons of substantial public interest as provided for in Article 9(g).

The ability to provide sufficient Derogations must be maintained in the UK for the processing of sensitive data where entering into an insurance contract, as noted in Theme 7 as a specific and new legal basis; *"the processing is necessary for the arranging, underwriting, and administration of insurance and reinsurance policies and insurance and reinsurance policy claims."* Such derogations can be implemented through Article 9(g) or through the continuance of:

> Statutory Instrument 2000 No. 417 (The Data Protection (Processing of Sensitive Personal Data) Order 2000) which allow insurers to process fraud, process certain health data without explicit consent (potentially enabled through Recital 10 or Article 9 (4) and further the recognition of principles in the Consumer Insurance (Disclosure and Representations) Act 2012, which allows an individual to act on behalf of, or as agent, and provide information on behalf of another in order to obtain insurance cover.

Article 15 - Right of access by the data subject – in relation to Member State Restrictions (Article 23):

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. UK Derogations are required to maintain existing provisions as set out in the Data Protection Act 1998 ("DPA") to ensure this process is executed within the boundaries of established protocols, namely, but not limited to;

- The maintenance of Confidentiality – DPA Section 7, (4), (5), (6)
- Limit excessive Data Subject Requests, which are determined to be disproportionate and excessive - DPA Section 7, (7)
- Comply with Member State Crime, National Security, Taxation, Fraud requirements and legal proceedings – DPA Section 29 & Section 35
- Comply with Health, Education and Social Work activity DPA Section 30
- Comply with Member State Regulatory Activity DPA Section 31
- Comply with Journalism, Literature and Art purposes – DPA Section 32
- Comply with Research and Statistical Purposes – DPA Section 33, as provided for by Article 89 (2).
- Comply with businesses and organisations requirements to maintain their confidentiality, and intellectual know-how DPA Schedule 7, (5) including negotiations DPA Schedule 7, (7)

- Comply with Legal professional privilege DPA Schedule 7 (10)

Article 17: - Right to erasure;

Adequate UK derogations are required to ensure the Data Controller complies with existing UK Statue in relation to legal retention requirements, and the necessity for establishment the exercise or defence of legal claims.

Theme 1 – Supervisory Authority

Supervisory Authority

Article 51 – Supervisory Authority
Article 53 – General Conditions for the members of the supervisory authority
Article 54 – Rules on the establishment of the supervisory authority
Article 58 – Powers
Article 59 - Activity report
Article 62 – Joint operations of supervisory authorities
Article 90 – Obligations of secrecy

Response: Article 58 – to ensure the Supervisory Authority (UK "Information Commissioner's Office, "ICO") maintains the current ability to agree undertakings with businesses to prompt changes within those organisations' policies and practices, and issue enforcement notices compelling organisational changes on its terms in favour of direct fines, should be maintained by issuance of a UK derogation.

Theme 2 – Sanctions

Sanctions

The derogations relating to sanctions include articles:

Article 36 – Prior consultation
Article 58 – Powers
Article 83 – General conditions for imposing administrative fines
Article 84 - Penalties

Response: Article 58 – See Theme 1 response.
Derogations should be upheld in the UK.

Theme 3 – Demonstrating Compliance

Demonstrating Compliance

The derogations relating to Demonstrating Compliance include articles:

Article 40 – Codes of Conduct
Article 42 – Certification
Article 43 – Certification Bodies

These Derogations should be upheld in the UK.

Theme 4 – Data Protection Officers

Data Protection Officers

The derogations relating to Data Protection Officers include articles:

Article 4 - Definitions
Article 37 – Designation of the Data Protection Officer
Article 38 – Position of the Data Protection Officer

Response: Article 4 – there is no definition of the Data Protection Officer within Article 4; if EU derogation enables a definition for a Data Protection Officer, this should be provided for by the Member State with consideration of the WP29 Guidance for Data Protection Officers, dated 5th April 2017.

Response: Article 37 - Derogation should be upheld in the UK.
Response: Article 38 –Derogation should be upheld in the UK.

Theme 6 – Third Country Transfers

Third Country Transfers

The derogations related to third country transfers include Article:

Article 49 – Derogations for specific situations.

Response: Article 49; These Derogations should be upheld in the UK.

Theme 10 – Processing of Children's Personal Data by Online Services

Processing of Children's Personal Data by Online Services

The derogation related to the processing of Children's Personal Data by Online Services includes Articles:

Article 8 – Conditions applicable to child's consent in relation to information society services.

Article 8 - The ability to provide by law for a lower age for those purposes provided by derogation should be upheld in the UK in relation to Online Services only.

Theme 11 – Freedom of Expression in the Media

Freedom of Expression in the Media

The derogation related to Freedom of Expression in the Media includes Articles:

Article 85 – Processing and freedom of expression and information

Article 85 - The ability to reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information provided by derogation should be upheld in the UK in line with the existing Data Protection Act 1998 provisions (Exemptions, Section 32).

Theme 12 – Processing of Data

Processing of Data

The derogation relating to the processing of data includes Articles:

Article 6 – Lawfulness of Processing
Article 18 – Right to restriction of Processing
Article 28 – Processor
Article 29 – Processing under the authority of the controller or processor
Article 32 – Security of Processing
Article 37 – Designation of the Data Protection Officer
Article 86 – Processing and public access to official documents
Article 87 – Processing of national identification number
Article 88 – Processing in the context of Employment

Article 6; Article 18(2); Article 28; Article 29; Article 32(4); Article 37; Article 86; Article 87; Article 88, in consideration of Article 9(2)(b) derogations should be upheld in the UK.