# Blog 6

# Lawful Processing

# Background

If you’ve read blogs 1 – 5 and cast around the GDPR Dropbox you’ll have come across the terms “lawfulness” and “legal justifications” and “Articles 6 & 9”. These are all references to Articles 6 and 9 of the original full text of the;

 **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 27 April 2016**

**on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**

Now original full texts are not the most interesting things nor always easy to understand. So here are those real original words but I’ve added my translation in the bold and blue above each section. I hope that is of use. Remember for special category data, i.e. health data, in order to lawfully process data there has to be both an Article 6 and an Article 9 justification. Please note para 1 of Article 9 where I’ve highlighted the key words in red, it confirms the default position for health data that is there should be no processing unless……

Article 6

Lawfulness of processing

FOR PROCESSING OF ANY DATA TO BE LEGAL ONE OF THE FOLLOWING MUST APPLY

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

THE PATIENT CONSENTS

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

THERE IS A CONTRACT INVOLVING THE DATA SUBJECTS

|  |  |
| --- | --- |
| (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; |

IT IS REQUIRED / ALLOWED / COMPLYING WITH A LAW (NOTE SUBJECT TO PARA 2 AND 3 BELOW AS WELL)

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

IT IS TO PROTECTING VITAL INTERESTS

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

IT IS IN PUBLIC INTEREST OR EXERCISE OF APPROPRIATE AUTHORITY (NOTE SUBJECT TO PARA 2 AND 3 BELOW AS WELL)

|  |  |
| --- | --- |
| (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; |

IN THE INTEREST OF DATA CONTROLLER OR 3RD PARTIES WITH CAVEAT SUBJECT TO OVERRIDING INTERESTS OF THE DATA SUBJECT

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

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

THE UK GOVENRMENTS CAN INTRODUCE ENHANCEMENTS TO (c) and (e) IN ARTICLE 6(1) IF THEY WISH

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.

(c) AND (e) ABOVE MUST BE BASED IN EU LAW

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 |

OR MEMBER STATE LAW

|  |  |
| --- | --- |
| (b) | Member State law to which the controller is subject. |

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

YOU CAN’T RE-PURPOSE DATA YOU POSSESS. YOU PROBABLY NEED TO RE-CONSENT. THINGS TO CONSIDER WHEN DECIDING TO RE-CONSENT OR NOT

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:

IS NEW PURPOSE SIMILAR TO ORIGINAL?

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

WHAT WAS THE CONTEXT?

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

THE TYPE OF DATA

|  |  |
| --- | --- |
| (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; |

THE CONSEQUENCES OF GOING AHEAD REGARDLESS

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

HOW SAFE IS THE DATA

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

Article 9

Processing of special categories of personal data

FUNDAMENTAL DEFAULT STARTING POSITION IS NO PROCESSING

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.

EXCEPT IF

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

THE DATA SUBJECT HAS CONSENTED

|  |  |
| --- | --- |
| (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; |

IT IS NECESSARY FOR EMPLOYMENT SOCIAL SECURITY AND SOCIAL PROTECTION LAW

|  |  |
| --- | --- |
| (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; |

IT PROTECTS THE VITAL INTERESTS OF SUBJECTS WHEN UNABLE TO CONSENT

|  |  |
| --- | --- |
| (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; |

WHEN PROCESSING IS DONE BY POLITICAL BODIES, RELIGIONS AND TRADE UNIONS

|  |  |
| --- | --- |
| (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; |

THE DATA IS ALREADY IN PUBLIC DOMAIN

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

WHEN IN OPEN COURT OR FOR LEGAL DEFENCE

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

NECESSARY FOR SUBSTANTIAL PUBLIC NTEREST, SUBJECT TO OBJECTION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| (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; |

NECESSARY FOR HEALTH CARE AND PREVENTION, PROFESSIONALS PROTECTED

|  |  |
| --- | --- |
| (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; |

PUBLIC HEALTH, SUBJECT TO DS RIGHT SAND PROFESSIONAL SECRECY

|  |  |  |
| --- | --- | --- |
| (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; |

RESEARCH

|  |  |
| --- | --- |
| (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. |

PROCESSING BY DOCTORS REGISTERED WITH GMC UNDER (2)(h) IS OK

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.

UK GOVERNMENTS CAN INTRODUCE ADDITIONAL LAWS GOVERNING THESE AREAS

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.

*Article 30*

**Records of processing activities**

1.   Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

|  |  |
| --- | --- |
| (a) | the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; |

|  |  |
| --- | --- |
| (b) | the purposes of the processing; |

|  |  |
| --- | --- |
| (c) | a description of the categories of data subjects and of the categories of personal data; |

|  |  |
| --- | --- |
| (d) | the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; |

|  |  |
| --- | --- |
| (e) | where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; |

|  |  |
| --- | --- |
| (f) | where possible, the envisaged time limits for erasure of the different categories of data; |

|  |  |
| --- | --- |
| (g) | where possible, a general description of the technical and organisational security measures referred to in Article 32(1). |

2.   Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

|  |  |
| --- | --- |
| (a) | the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; |

|  |  |
| --- | --- |
| (b) | the categories of processing carried out on behalf of each controller; |

|  |  |
| --- | --- |
| (c) | where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; |

|  |  |
| --- | --- |
| (d) | where possible, a general description of the technical and organisational security measures referred to in Article 32(1). |

3.   The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4.   The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5.   The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.