T.H.I.N.C.S
TONY HELLIWELL
INSURANCE NURSE CONSULTANCY SERVICES LTD

Introduction: GDPR Lawful Basis Background

Companies subject to the EU General Data Protection Regulation (GDPR) may justify processing activities based on one of six categories. GDPR states that you should assess the basis on which you are processing data. Processing shall be lawful only if and to the extent that at least one of the following applies:

1. The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
2. 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;
3. processing is necessary for compliance with a **legal obligation** to which the controller is subject;
4. processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
5. 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;
6. 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

When considering option 6 it is important to recognise that the phrase “legitimate interests” is not a defined in the GDPR and this one phrase has probably generated more discussion than any other.

The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

The use of legitimate interest needs careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the

data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

Also, the controllers' legitimate interests in many cases appears to overlap with other legal bases for processing. GDPR acknowledges that controllers have a legitimate interest in processing needed to ensure security of networks and information systems, but this processing can also be justified as a being a task carried out in the public interest. Similarly, processing data for public health purposes might be done both as a legitimate interest of the controller and because it is necessary to protect the vital interests of the data subject.

GDPR Definition of Processing Activities Justified by Legitimate Interests

From the GDPR's guidance, the following types of processing activities may be justified on the basis of legitimate interests:

Processing of customer or client data, including for direct marketing

Where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. Provided that the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

Any assumption that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest needs very careful consideration and thorough documentation.

Processing of data to the extent strictly necessary for network and information security

The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security,
i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services.

Certain *ad hoc* data transfers

Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data.

Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

Assessing and Documenting Legitimate Interests

It is important to note that merely having a legitimate interest is not sufficient to justify the processing activities; the legitimate interest must not itself by outweighed by the rights and freedoms of the data subject. Controllers must consider if the data subject has a right to object to the processing.

Where personal data might lawfully be processed because 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, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

Additionally, as is clear from the GDPR, prior to relying on a legitimate interest as a basis for processing, the controller must undertake an assessment to determine

1. whether the data subject would reasonably expect the processing (given the context of the collection of the data)

2. whether the legitimate interest is overridden by the rights of the data subject. The implication from the guidance is that, should the processing not be reasonably expected, the rights and freedoms of the data subject may well prevail. (“The interests and fundamental rights of the data subject could

in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.")

A number of options exist for this assessment. One widely accepted approach is based on work completed by the Data Protection Network. This can be found at:

https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/