GDPRG04 - Processing Personal Data

9th February 2018

GDPR - Processing Personal Data

Under both the Data Protection Act 1998 and the General Data Protection Regulation 2016 ("GDPR") organisations must ensure there is a lawful basis for processing personal data. If there is no lawful basis for processing, the processing should not take place.

This expert insight focuses on some of the grounds for processing that are most likely to apply to organisations in the health and care sector, including:

1. Consent from the data subject
2. Legitimate interest of the Data Controller or a third party
3. Performance of a contract
4. Protection of the vital interests of a data subject
5. In the case of special categories of data:

    a. Processing in the field of employment; and

    b. Processing for the provision of health or social care or treatment or the management of health or social care systems and services.

1. Consent

If none of the other grounds applies to the processing of personal data, organisations must obtain express consent from the data subject to process their personal data.

For example, in some circumstances, marketing communications can only be sent to a data subject if the data subject has given their express consent to receiving the communications. This will apply if marketing communications are sent to individuals to whom the organisation does not provide services. If an organisation wishes to send marketing communications to its current customers and clients, it is likely that it will be able to rely on the grounds of legitimate interest for doing so, although the Information Commissioner's Office is still to confirm that point.

Consent should also be sought if an Employee's personal data is processed for a reason other than usual HR/Administrative purposes. This will need to be considered on a case by case basis but may include, for example, contacting an employee on their personal phone for work purposes.

Under GDPR, consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The statement above means that consent must relate specifically to the purpose for which the organisation wishes to process the personal data and the giving of consent must be a positive action. Implied or negative consent (including, for example, pre-ticked boxes often used to sign up for marketing communications) will no longer be sufficient.

2. Legitimate Interest (Art 6.1(f))

At a high level, legitimate interest means the data subject would reasonably expect an organisation to process its data in the manner it is being processed.

This will apply, for example, to the processing by an organisation of employee data for HR/Staff purposes. There is no need to obtain consent from each employee for their personal data to be processed.

Legitimate interest will apply to much of the ancillary processing of personal data carried out by organisations, for example, processing the individual names and email addresses of contacts at business suppliers.

It will also apply to processing contact details of a person to whom an organisation provides services – for example, it is in the legitimate interests of a care service to process the service user's name, contact information and next of kin. This may also be permitted on the grounds of fulfilment of a contract – see below for more information.

Legitimate interest will not apply where the interests of the organisation are overridden by the interests, rights or freedoms of the data subject. It also does not apply to public authorities (but it can be relied upon by health and care organisations in the independent sector).

3. Performance of a Contract (Art 6.1(b))

Organisations are entitled to process personal data without obtaining consent to the extent the processing is necessary to perform a contract.

If a care home enters into a contract to provide care to a service user, GDPR recognises that certain personal data will need to be processed to fulfil the contract and provide the services. The types of personal data that may be processed on this basis will depend on the services being provided and the contract in place.

4. Protection of the Vital Interests of a Data Subject

For this ground to apply, the processing must be necessary to protect an interest which is essential for the life of the data subject or another person. It is therefore very limited in scope and will only apply to a life and death situation i.e. the provision of emergency medical care. If the individual is capable of giving consent to the processing, the vital interests ground won't apply – consent must be sought.

GDPRG04 - Processing Personal Data

5. Special Categories of Data (Art 9)

The grounds that apply to the processing of special categories of data differ to those which apply to the processing of other personal data.

In many situations, explicit consent will be required. However, there are a number of other grounds which may apply to organisations in the health and social care sector and which mean consent does not need to be obtained:

(i) Processing Necessary in the Field of Employment

Organisations are able to rely on this ground to process special categories of data to the extent such processing is necessary for usual Employment/HR Purposes. This may include, for example, recording on an employee's file any health issues that may affect their ability to work or of which the organisation needs to be aware. Organisations will need to consider their processing of special categories of personal data for HR purposes on a case by case basis. One example provided by the ICO of processing that may not be captured by this ground is the processing of special categories of data for the purposes of carrying out an occupational health assessment. In this scenario, consent would need to be obtained from the data subject.

(ii) Processing Necessary to Protect the Vital Interests of the Data Subject or Another Natural Person

The same principles apply as those set out above in respect of non-sensitive types of personal data. This ground can only be relied upon in cases of life and death (of the data subject or another person) where the data subject is incapable of giving their consent.

(iii) Processing Necessary for the Purposes of Preventive or Occupational Medicine, for the Assessment of the Working Capacity of the Employee, Medical Diagnosis, Provision of Health or Social Care or Treatment or the Management of Health or Social Care Systems and Services

GDPR expands the grounds upon which special categories of data can be processed for health and social care reasons. The provision of "health or social care or treatment" is now expressly referred to, which means where personal data is being processed to facilitate the provision of such care or treatment, there is no need to obtain express consent from the data subject.

GDPR requires, however, that where processing takes place on the ground referred to at (iii) above, there must be "obligations of professional secrecy" (i.e confidentiality obligations) in place.

Fair Processing Notices

Organisations must provide fair processing notices to all individuals whose personal data is processed. The notices include the grounds upon which processing is carried out. This allows an organisation to communicate unambiguously the lawful basis of processing and indicate the types of processing involved. An organisation may have more than one fair processing notice, for example, one for service users, one for relatives and one for suppliers.

GDPRG04 - Processing Personal Data

Privacy and Electronic Communications Regulations 2003 (“PECR”)

PECR sits alongside the Data Protection Act 1998 and GDPR. It is currently in the process of being updated and the final draft has not yet been finalised. PECR (and its replacement) focus on the sending of electronic communications (i.e. by email, text & phone) and must be complied with in addition to GDPR.

PECR is particularly important for organisations that send marketing communications by email or by text. If you fall into this category, you should ensure you understand and comply with the principles of PECR and that you keep up to date with the reform of PECR. You can find more information here - https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/.

Further Reading

All grounds that apply to the processing of personal data are set out in Article 6 of GDPR and the grounds that apply to special categories of data are contained in Article 9. The full text of GDPR can be found here https://gdpr-info.eu/

Note: All QCS Policies are reviewed annually, more frequently, or as necessary.