Why you may not be processing Special Category personal data lawfully in the UK

Rocio de la Cruz, Principal Associate with Gowling WLG, explains what UK organisations, and organisations subject to the Data Protection Act 2018, must do to comply with the requirements for processing Special Category personal data

Over the last years, we have seen organisations seeking to comply with the General Data Protection Regulation ('GDPR') through building data maps which enable better understanding of issues such as the types of personal data they process, the reasons why they process personal data, and the methods used to obtain information. Such data maps may also throw light upon the manner in which data are shared with other parties, whether all data collected by default is essential to fulfil an identified purpose, and the appropriate legal basis for the processing to meet the GDPR's lawfulness principle.

When it comes to the processing of Special Category personal data as defined in Article 9 of the GDPR, organisations have been required to consider the application of Article 9. In doing so, they have sought to determine whether consent is the appropriate ground for their data processing. In some instances, the conclusion has been 'no' — particularly if any of the other derogations set out in Article 9 applies to the processing in question. In such cases, organisations have completed their data map and informed individuals accordingly.

However, organisations risk breaching the lawfulness requirement of the first GDPR principle if they only look at Article 9 of the GDPR to find a legal basis to process Special Category data, without considering the application of domestic law. In the UK, and for those organisations to which the UK Data Protection Act 2018 ('the DPA') applies due to its extraterritorial effect, Article 9 should be read along with Schedule 1 of the DPA to ensure that all mandatory requirements are met.

This article considers the GDPR and the DPA from the perspective of how they affect the assessment of the legal basis to process Special Category data and recommends the steps that organisations should consider to ensure the lawfulness of their processing activities.

The initial step: applying Articles 6 and 9 of the GDPR

First of all, it is important to note that Article 6 always applies (Article 6 lists the grounds for lawfully processing ordinary personal data). Hence, there will always be a need to find a legal basis in Article 6 for any processing activity, irrespective of the category of data that the company uses.

There are multiple grounds in Article 6, including that the processing is necessary for the company to fulfil a legal requirement or to fulfil the company's contractual obligations in agreements with data subjects.

To process Special Category data, a controller must find a legal basis for the processing activity in Article 6 of the GDPR *in addition to* a valid processing reason in Article 9 of the GPPR. For example, if a company wishes to carry out a survey to customers in which it is necessary for the purpose to identify customers and to collect data concerning their health condition, the company might conclude that it has a legitimate interest in carrying out this survey which is not overridden by their customers' interests (Article 6) and that it also needs explicit consent since Special Category data are involved in the project (Article 9) and none of the other Article 9 derogations is suitable for their project.

Looking for additional requirements under the DPA

Once UK organisations are satisfied that at least one of the grounds in Article 6 and one of the processing reason in Article 9 applies, the necessary further step is considering whether additional measures or requirements are required under the relevant local law.

When looking at the list of Article 9 derogations, it is crucial to note that some of them are subject to 'authorisation by Union or Member State Law'. These are where the processing is necessary:

- in the field of employment, social security or social protection law;
- for reasons of substantial public interest;
- for preventive or occupational medicine, health or social care;
- for reasons of public interest in the area of public health; or

(Continued on page 10)

(Continued from page 9)

- for archiving purposes in the public interest, scientific or historical research or statistical purposes.

As expected, all of the above grounds have been authorised by the DPA. However, the UK Act adds different requirements depending on the applicable legal ground. For example, considering what is and is not in the substantial public interest is not at the discretion of the controller only, since the 'substantial public interest' conditions (and the requirements to meet each of them) are set out in Part 2 of Schedule 1 of the DPA.

Another example is interpreting what constitutes 'health' or a 'social care' purpose, which is further defined in section 11 of the DPA. The exception should only be applied if all the requirements set out in Schedule 1, Part 1, paragraph 2 of the DPA are addressed. The same applies for those carrying out research and in need of processing Special Category data, who to properly assess the legal basis will need to consider the application of the GDPR (including Article 89) along with section 19 and Schedule 1, Part 1, paragraph 4 of the DPA, or otherwise find a different legal ground.

The obligation to put in place an 'appropriate policy document'

One of the requirements applied to most of the legal conditions stated in the DPA 2018 is to put in place an 'appropriate policy document' (the 'Appropriate Policy') and 'additional safeguards' as defined in Part 4 of Schedule 1 of the Act. The Appropriate Policy is an internal document documenting how the controller is complying with the law when relying on an Article 9 exception justifying the processing of the Special Category data. The Policy needs to explain how each of the data protection principles will be addressed — for example, how the use of that Special Category data will be fair to the individuals concerned; how the organisation will ensure transparency, data minimisation, accuracy, storage limitation and confidentiality. In addition, the Appropriate Policy should contain information on how long data are to be retained, as well as an explanation of the routines for erasure and retention. The Act states that the Appropriate Policy should be created when the controller begins using the Special Category data, and saved for at least six months after the processing activity has stopped.

Sample checklist: The collection of data concerning ethnic origin

Please complete this checklist to assess whether you can ask for data related to ethnic origin for this project, and send it to [our DPO/Legal] for approval.

Processing of ethnic origin within the field of employment:

— — — — — — — — — — — — — — — — — —

Do you need to process the data about ethnic origin in order for our company to comply with a legal requirement in connection with employment? If yes, please explain what the legal requirement is:

— — — — — — — — — — — — — — — — — —

Do you need to process the data about ethnic origin in order to comply with a law that is enforced on the data subject in connection with employment? If yes, explain the reason why:

— — — — — — — — — — — — — — — — — —

If you have answered yes on any of the above questions, are the above reasons already covered in any of our Appropriate Policies and our records of processing activities? Yes/No

— — — — — — — — — — — — — — — — — —

If you have answered no, please be aware that additional documentation will need to be in place before this data are collected.

The need for additional safeguards

In addition to the Appropriate Policy, the DPA requires controllers to include information on which condition the processing activity relies on, which legal ground (in Article 6 of the GDPR) the processing is based upon, and why this is appropriate. The controller should also state whether the routines for erasure which are indicated in the Appropriate Policy are being followed. If not, the controller should document the reason for the non-compliance.

The five steps to implement this in your organisation

Organisations processing Special Category data should consider the following:

Review data maps and records of processing activities: The very first step is to revise the data map and records of processing activities in place, to confirm that firstly that the legal grounds applied at the time are still appropriate, and secondly, what (if any) additional measures need to be in place to address all the DPA requirements.

Produce additional documentation as required under the DPA, and include them in the current set of internal policies: Once an Appropriate Policy is in place for each of the legal grounds the organisation is relying on, these should be aligned and cross-referenced with the group/company's data protection policies.

Help employees to avoid breaches: For the purposes of risk management and resource-planning, it is vital that central management is engaged and informed. Controllers may use checklists based on each of the DPA legal grounds and include them in the Appropriate Policies, after which staff should be informed and trained accordingly. Examples of checklists that are based on DPA requirements are included on pages 10 and 11. The

examples assume that a business function within a company is considering the processing of Special Category personal data for a new purpose. They are drafted as if they will be a new section within an existing policy document (for example the group/company's data protection policy, or a standalone policy for the processing of Special Category data). The idea is that when the business function consults the document, it will be able to provide the DPO or legal department with the information that the latter will need to consider whether or not the relevant DPA legal ground applies.

Update privacy notices: In order to be fair to data subjects and ensure transparency, organisations must document the legal basis being relied upon. It is therefore essential to review privacy notices regularly, and in particular if, as a result of a data map review exercise, the organisation has concluded that it needs to apply different legal grounds.

Involve data processors and joint controllers: So that they are aware of any additional rules and measures that have been implemented, organisations should consider providing copies of approved Appropriate Policies to any processors or joint controllers. Ideally, these will be added to data processing agreements or data sharing protocols as a set of additional binding rules.

Sample checklist: Collection of genetic data for health care purposes

Please complete this checklist to assess whether you can ask for data related to genetic data for this project, and send it to [our DPO/Legal] for approval.

Is the processing of genetic data necessary for any of the below purposes? Yes/No. If Yes, please explain the reason why:

— —

Preventative or occupational medicine [include example relevant to the business]

— —

The assessment of the working capacity of an employee [include example relevant to the business]

— —

Medical diagnosis [include example relevant to the business]

— —

The provision of health care or treatment [include example relevant to the business]

— —

The provision of social care [include example relevant to the business]

— —

The management of health care systems or services or social care systems or services [include example relevant to the business]

— —

Is the service being carried out by or under the responsibility of a health professional or a social work professional or by another person who owes a duty of confidentiality under an enactment or rule of law? Yes/No

— —

If you responded no to the last question, is it possible to collect the consent of individuals involved before the genetic data is obtained? Yes/No

— —

If you responded yes to the last question, how, in your opinion, we will be able to collect consent?

— —

Rocio de la Cruz
Principal Associate
Gowling WLG
Rocio.delaCruz@gowlingwlg.com