Croner

HR • Tax • H&S • Reward

Understanding the General Data Protection Regulations

Expert View - By Liam Holland

Croner

HR • Tax • H&S • Reward

Preparing for the General Data Protection Regulations (GDPR)

On May 25 2018, the European Union's General Data Protection Regulation (GDPR) is due to come into force, which will bring in a strict set of new rules concerning privacy and data security, and impose penalties on organisations which violate them.

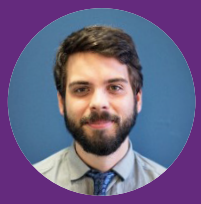
UK organisations that process the personal data of EU residents have only a short time to ensure that they are compliant. The regulations have been introduced to adapt to the pace of a modern digital landscape, and will be more extensive in scope and application than the current Data Protection Act.

This White Paper, written by Legal Advisor Liam Holland, aims to explain what GDPR is, how it will impact organisations, and the consequences of any breach.

Our comments and research within this report are intended as a guide for employers. For further advice or guidance on the matter, please contact **0800 032 4088.**

Contents

About The Author



Liam Holland
Croner Commercial Legal Advisor

With a particular interest in Company Law and Intellectual Property Law, and especially how the latter interacts with modern technology and forms of communication, Liam has practiced as a Legal Advisor for more than five years.

Prior to his legal career, Liam studied company law, legal practice, and economic legal theory - taking economic principles and applying to contractual and criminal legal foundations.

1. Principles and Grounds for Processing

The Data Protection Act 1998 sets out eight data protection principles. These principles will be used by the Information Commissioner's Office to guide their decision-making when it comes to enforcement action. Much like the Data Protection Agency, the General Data Protection Regulations (GDPR) have a set of guiding principles, under Article 5.

The principles say personal data should be:

- Processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency')
- Processed no further than for the legitimate purposes for which the data was collected ('purpose limitation')
- Limited to what is necessary in relation to the purpose ('data minimisation')
- Accurate and kept up to date ('accuracy')
- Kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation')
- Processed in a manner that ensures security of that personal data ('integrity and confidentiality')
- Processed by a data controller who can demonstrate compliance with the principles ('accountability')

You will see these principles referred to in later chapters. It is worth noting that the Information Commissioner's Office does take a view, when there has been an alleged data breach, on the extent to which the data controller or data processor have complied with these principles.

While they will always look at whether the letter of the law has been broken - they will also look at whether the data controller or data processor in question have demonstrated that, at the very least, they have considered the above principles.

In addition, they must demonstrate that their decision was an informed one which takes into account a data subject's rights to the fullest extent possible in any given set of circumstances.

While many of the above principles will appear and be referred to later, it is worth taking particular note of the lawfulness, fairness and transparency principle. This primarily refers to the justification on which a data controller relies to allow them to process personal data.

Under Article 6 of the GDPR, there is a list of grounds where it is lawful to process personal data. This is very similar to the list of justifications for processing under

the Data Protection Regulations, Schedule 2.

There are six grounds for processing personal data, but we would suggest there are three 'main' grounds under which the majority of processing will fall. These are:

- Consent
- Processed no further than for the legitimate purposes for which the data was collected ('purpose limitation')
- The processing is necessary for the purpose of a legitimate interest pursued by the data controller

We intend to go into further detail on consent in a later chapter, but with regard to the other two grounds for processing referenced above, we would urge employers to pay particular attention to the words 'necessary' and 'legitimate'.

For processing to be necessary, it must be more than just beneficial or convenient. Likewise, legitimate means something more than 'would like to', so there must be an underlying interest which the data controller is entitled to pursue.

The grounds for processing special categories of personal data (which is much the same as sensitive personal data under the Data Protection Regulations) are set out under Article 9 of the GPDR.

2. Consent

Under the General Data Protection Regulation (GDPR), the definition of consent has changed and has caused some consternation from interested parties from all areas of industry.

Under the Data Protection Act 1998, consent was never defined within the body of the text. It was interpreted in line with the Data Protection Directive as meaning:

> “ Any freely-given specific and informed indication of the [data subject's] wishes by which the data subject signifies his agreement…

Consent was one of the conditions for processing under the Data Protection Regulations' Schedule 2. Under the GDPR consent is defined within the Regulations themselves and means:

> “ Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement…

Much like the conditions for processing under Schedule 2 of the Data Protection Regulations, consent is one of the grounds for lawful processing under Article 6 of the GDPR (despite the terminology change, these are much the same thing).

Part of the consternation comes from the requirement for a 'statement' or 'clear affirmative action'. This requirement for it to be a positive action by the data subject may mean that data controllers have to review how they collect information on data subjects - rather than relying on a pre-filled tick boxes. For example, data controllers will have to ask the data subject to positively agree (by positively ticking a box for example).

The other issues with consent are that if consent is the ground for lawful processing relied upon by the data controller, this gives the data subject enhanced rights over that data over some of the other grounds for lawful processing.

Further, where consent is the grounds relied upon for lawful processing, the data subject always has the right to withdraw consent.

Finally, consent will not be valid, as it will not be 'freely-given' where a contract is conditional upon consent to process it. I am therefore of the view that many contracts will need to be rephrased to make it clear that the grounds for lawful processing are that it is necessary for the performance of a contract to which the data subject is a party.

One could argue that changing the condition for processing from 'consent' to 'performance of a contract to which the data subject is a party' could be seen by some as a poor use of their time.

I would disagree, as ultimately, on nearly all facets of the GDPR, it is for the data controller to demonstrate compliance, to the extent that this is one of the guiding principles of the GDPR.

This would mean that a data controller is open to criticism for not providing the data subject with certain information including their lawful grounds of processing and not being transparent in their dealings with data subjects.

Let's assume the data controller manages to convince the Information Commissioner's Office that the consent was valid, in which case the data subject now has enhanced rights over that data.

Given the above, it is more important than ever that a data controller establishes the correct grounds for processing from the outset and has an appreciation for the rights of the data subject, which 'attach' to these grounds.

3. Information Requirements

As previously discussed, the Data Protection Act 1998 requires an organisation to ensure there is justification for any processing - with a list of the relevant conditions being set out in Schedule 2.

Under the Data Protection Act, once you have this 'justification', the data controller is then free to process the data, albeit in line with the other principles of the Data Protection Act. Ultimately however, the data controller does not have to inform the data subject that information about them is being processed.

Article 13 of the General Data Protection Regulation (GDPR) introduces a new requirement on a data controller to provide certain information to a data subject when personal data is collected from that data subject.

This information must be provided to the data subject when the personal data is collected, but the regulations are not prescriptive as to how this information should be provided, merely that it should be.

In summary, the information which a data controller has to provide a data subject with, is as follows:

- The identity and the contact details of the data controller and, where applicable, of the data controller's representative
- The contact details of the Data Protection Officer, where applicable
- The purposes of the processing for which the personal data is intended, as well as the legal basis for the processing
- If applicable, the legitimate interests pursued by the controller or by a third party
- The recipients or categories of recipients of the personal data, if any
- Where applicable, the fact that the data controller intends to transfer personal data to another country or international organisation
- The existence or absence of a ruling by the Commission on the adequacy of Data Protection laws in any given jurisdiction or international organisation
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request from the controller access to and rectification or erasure of personal data, or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with a supervisory authority

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract. They must also provide information on whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

- The existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

It is worth noting that where the data controller intends to process personal information for a purpose other than that for which the personal data was collected for, then the data controller needs to provide the data subject with the information relating to that further purpose.

Under Article 14 of the GDPR where a data controller has obtained personal data about a data subject from a source which is not that data subject then, within one month of receipt of that information, the data controller must provide to the data subject the same information.

They must also include information about the categories of personal data being processed and information about the source of the personal data, and whether this is publicly accessible. There are exemptions to Article 14, primarily where there is a statutory obligation of secrecy.

4. Data Subject Rights

Aside from the right to information under the General Data Protection Regulations (GDPR), data subjects have other rights, some of which are the same, or similar to, those contained within the Data Protection Act 1998. Some of which are new.

Under Article 15 of the GDPR, a data subject has the right to access the data which a data controller holds about him or her. The data controller must, upon receipt of a request, confirm the following:

- The purpose of the processing
- The categories of the personal data being processed
- The recipients to whom personal data has, or will be, disclosed
- The retention period relating to that data
- The existence of the right of rectification or erasure (discussed below)
- The right to lodge a complaint with the Information Commissioner's Office
- The source of the information (where this is not the data subject)
- The existence of any automated decision making

Furthermore, the data controller should provide a copy of the information to the data subject. This is similar to a Subject Access Request under the Data Protection Act: albeit no fee may now be charged except an administrative fee for further copies. The time limit for responding to this request will be one month, rather than the 40 days to respond to a Subject Access Request.

Data subjects also have the right of rectification, which means the right to request that inaccurate data held about the data subject is corrected.

The GDPR also contains a right to erasure, more commonly known as the right to be forgotten. This right effectively entitles a data subject to request that a controller erase all data held regarding that data subject where one of the grounds apply.

The grounds are:

- The personal data is no longer necessary in relation to the purpose for which it was collected
- The data subject has withdrawn their consent for the data controller to process the data
- Where the data subject has the right to object to data processed for direct marketing or where there is no longer a legitimate interest of the data controller in processing the data
- The data has been processed unlawfully
- It is required to be erased for compliance with a legal obligation
- The personal data has been collected in relation to the offer of information society services. This is any information society service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

The controller does not have to comply with the right to erasure where the processing is required for compliance with a legal obligation, or where the data is processed in relation to a legal claim.

The data subject has the right to restrict processing of personal data where:

- The accuracy of the data is contested by the data subject
- The processing is unlawful but the data subject opposes erasure but requires restriction instead
- The data controller no longer needs the data but it is required by the data subject for a legal claim.

Restricted processing means the data controller may only store, or further process, with the consent of the data subject, or for legal claims.

With regard to the right of restriction and erasure: the controller is required to notify any other party to whom the data has been disclosed of any data in respect of which the subject has requested either a restriction or erasure.

The data subject also has the right to 'data portability'. Data portability requires the data controller, upon request from the data subject, to provide to the data subject (or any other data controller identified by the data subject) any personal data concerning the data subject, which has been provided by the data subject themselves.

The data must be given in a structured, commonly used and machine readable format. This right only applies where the data controller has relied upon consent as their reason for processing or the processing is carried out by automated means.

5. Controllers and Processors

Under the Data Protection Act 1998, there were two categories of persons, natural or legal, which processed data - data controllers and data processors. Under the General Data Protection Regulations (GDPR), these two categories still exist, albeit now defined simply as controllers and processors.

The GDPR defines a **controller** as

> “ the natural or legal person…which alone, or jointly with others, determines the purposes and means of the processing of personal data…

A **processor** ‘means a natural or legal person…which processes personal data on behalf of the controller’.

This can generally be summarised as meaning the controller is the person/organisation which ‘owns’ the data, and the processor is a person/organisation that processes data for the controller.

It should generally be assumed that the GDPR applies to ‘a controller’ in its entirety, just as it did under the Data Protection Act.

Processors were never directly bound by the Data Protection Act, but under the GDPR processors are directly bound by certain provisions of the GDPR - the majority of which are set under articles 28 to 37.

Controllers are obliged to only appoint processors who provide sufficient guarantees to have in place appropriate technical and/or organisational measures to ensure processing meets the requirements of the GDPR.

Furthermore, processors are required by the regulations to carry out such processing in accordance with the controller’s instructions. These requirements are intentionally vague and broad, and effectively impose an obligation on the processor to comply with many of the requirements of the GDPR (such as adequate security, data minimisation etc), albeit on the controller’s instruction.

It is likely that these instructions will be included as part of any contract applicable between a controller and a processor.

Processors will also require specific consent of the controller in order to sub-contract any of their duties. While this consent could certainly be contained within the contract between the controller and processor, even where consent is given, the processor must inform the controller of any new sub-contractor - effectively giving the controller time to object to the appointment of any particular sub-contractor. Any sub-contractor must be contractually bound to the same, or similar, obligations as the ‘main’ processor.

The processor, and the controller, must maintain a record of their processing activities, the content of which is set out under article 30 of the GDPR, and this record must be made available to the Information Commissioner’s Office upon request.

Generally speaking, alongside the specific provisions above, a processor should also be complying with the spirit of the principles set out in the GDPR.

6. The Role of a Data Protection Officer

The concept of the Data Protection Officer is a new concept in UK law, but one which is commonplace in some European Union States.

Under the General Data Protection Regulations (GDPR), certain controllers and processors will be required to appoint a Data Protection Officer.

If a controller or processor is required to appoint a Data Protection Officer then they are under a duty to ensure the Data Protection Officer is properly involved in all issues which relate to the protection of personal data.

A controller or processor is required to appoint a Data Protection Officer where:

- It is processing personal data and is a public authority, except for the courts acting in a judicial capacity
- The core activities of the controller or processor consist of operations, which by their nature, their scope or their purpose, require regular and systemic monitoring of data subjects on a large scale
- The core activities of the controller or processor consist of the processing of special categories of personal data or criminal convictions on a large scale.

Even if there is no requirement to have a Data Protection Officer, a controller or processor may elect to appoint a Data Protection Officer in any event.

A group of undertakings may appoint a single Data Protection Officer to act across the group provided that the Data Protection Officer is easily contactable from each part of the group.

The Data Protection Officer may be an employee of the controller or processor, or may be on a service contract. The Data Protection Officer should have expert knowledge of data protection law and practices, and the controller or processor must publish the contact details of the Data Protection Officer and inform the Information Commissioner's Office of their details.

The Data Protection Officer may not, under any circumstance, be penalised or dismissed as a result of carrying out their tasks as the Data Protection Officer and must be given adequate resources to perform the role.

Furthermore, the Data Protection Officer must report to the highest levels of management of the controller or processor.

As a bare minimum, the Data Protection Officer must carry out the following tasks:

- To inform the controller or processor, and their employees, of their obligations under data protection laws
- Monitor compliance with data protection laws and the controller or processor's own policies, including assignment of responsibilities, raising awareness and the training of staff
- To provide advice on data protection impact assessments and monitor the performance of the data protection impact assessments
- To cooperate with the Information Commissioner's Office
- To act as a contact point for the Information Commissioner's Office.

7. Breach Notification and Sanctions

Under the Data Protection Act 1998 there is no mandatory obligation to notify the Information Commissioner's Office of a data breach, albeit the Information Commissioner's Office did expect controllers to self-report where there was a sufficiently serious breach.

Self-reporting in such cases was often useful to demonstrate to the Information Commissioner's Office that the data controller was attempting to deal with such matters in a good faith manner in accordance with the spirit of the Data Protection Act.

The General Data Protection Regulations (GDPR) define a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

As one can see from the above definition, a personal data breach is therefore far wider than simply meaning unauthorised disclosure to a third party.

Under Article 33 of the GDPR, a controller is obliged to notify the Information Commissioner's Office of any personal data breaches within 72 hours of the breach taking place, unless the personal data breach is unlikely to result in a 'risk to the rights and freedoms of natural persons'.

Note that if a risk exists, it can be to someone other than the data subject and, as such, the controller would be required to notify the Information Commissioner's Office. What exactly is meant by 'a risk to the rights and freedoms of natural persons' is likely to be a highly contested area.

The notification of the breach to the Information Commissioner's Office must contain the following information:

- A description of the nature of the personal data breach, including the number of data subjects concerned and the categories and number of personal data records concerned
- The name and contact details of the controllers Data Protection Officer or other contact point
- A description of the likely consequences of the personal data breach
- A description of the measures taken by the controller to address the breach, including any measures to mitigate the risk(s) to the data subject(s).

The controller is also obliged to document any data protection breaches including the facts relating to the breach, its impact, and any remedial action taken by the controller.

Where a processor becomes aware of a personal data breach, the processor is obliged to inform the controller without undue delay.

There is also an obligation on the controller to notify the data subject of a personal data breach, but only where the breach 'is likely to result in a high risk to the rights and freedoms of natural persons…' without undue delay.

While again it is unclear what is meant by a 'high risk', the threshold is clearly higher than the obligation to notify the Information Commissioner's Office which requires notification, unless the breach 'is unlikely to result in a risk'.

The notice to the data subject must contain broadly the same information as a notice to the Information Commissioner's Office under Article 33.

Sanctions

Any breach of the GDPR carries potentially hefty penalties by way of fines imposed by the Information Commissioner's Office which, depending on the nature of the infringement, could be up to 20 million euros or up to 4% of worldwide annual turnover, whichever is the higher.

Furthermore, a data subject has the right to lodge a complaint with the Information Commissioner's Office and has the right to 'an effective judicial remedy'. We can therefore expect, much like with the Data Protection Officer at this time, that data subjects will be able to recover financial loss and potentially a sum of money for distress.

Let's talk

PHONE 0800 032 4088
ONLINE croner.co.uk

Croner Group Limited registered
in England & Wales,
No. 8654528.
Registered Office:
Croner House,
Wheatfield Way,
Hinckley, LE10 1YG.

What We Do

HR & Employment Law
Advice & Consultancy
Employee Assistance Programme
Case Management Software

Health & Safety
Advice & Consultancy
Training Courses
Risk Management Software

Pay & Benefits
Salary Benchmarking
Consultancy
Job Evaluation Software

Croner
HR • Tax • H&S • Reward

2017 Trusted Service Awards
feefo

best company 'one to watch' 2017

TRUSTPILOT