DATA PROTECTION

# A GUIDE FOR EMPLOYERS

HART BROWN

SOLICITORS

Protecting people's rights when processing their personal information has always been important but a recent overhaul in the law regarding data protection has made businesses more aware of its impact. The GDPR (General Data Protection Regulation) is concerned with protecting the rights of individuals when processing their personal information and is contained within UK law through the Data Protection Act 2018.

It is a complex area and communicating how you handle data to your employees by having in place effective data handling policies and procedures is key. All employees need to be made aware that they have a duty to ensure that their activities at work comply with the data protection principles below.

## EIGHT PRINCIPLES OF THE GDPR

### The handling of personal data must follow the relevant principles below : -

| | | |
|---|---|---|
| PRINCIPLE ONE | **Lawful** | Processed fairly, lawfully and in a transparent manner in relation to the data subject. |
| PRINCIPLE TWO | **Limited for its purpose** | Adequate, relevant, limited to what is necessary in relation to the purposes for which they are processed. |
| PRINCIPLE THREE | **Data minimisation** | Data collected must be necessary and not excessive for its purpose. |
| PRINCIPLE FOUR | **Accurate** | Accurate and, where necessary, kept up to date. |
| PRINCIPLE FIVE | **Retention** | Kept in a form that permits identification of data subjects are no longer than is necessary for the purposes for which the personal data are processed. |
| PRINCIPLE SIX | **Integrity and confidentiality** | Processed in a manner that ensures appropriate security of the personal data including protection against an authorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. |
| PRINCIPLE SEVEN | **Data security** | Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. |
| PRINCIPLE EIGHT | **Transfers outside of EU** | Personal data shall not be transferred to a country or territory outside the European economic area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. |

**It is not enough just to comply with all of these principles; you must show how you comply with them. This means having updated policies about how personal data is managed and making sure that there is a clear compliance structure, responsibilities are allocated to staff, staff are trained and systems have been audited. It also means bringing in technical measures to improve safety and security; and ensuring individuals can properly access their data.**

## LEGAL BASIS FOR PROCESSING DATA

### Use of any personal data under the GDPR must be justified using one of the following conditions for processing :-

| | |
|---|---|
| **Consent** | Must be able to demonstrate that an individual gave their consent to the processing and must be able to withdraw consent. |
| **Contract** | Performance of a contract. |
| **Legal obligation** | Compliance with a legal obligation that does not include a contract. |
| **Medical situation** | To save someone's life. |
| **Public function** | To carry out a public function. |
| **Legitimate Interest** | Processing is necessary for the purposes of a legitimate interest pursued by the data controller or by a third-party, except where such interest or overridden by the interest of fundamental rights and freedoms the data subject which requires protection of personal data, in particular where the Data subject is a child. |

## SUBJECT ACCESS REQUESTS

Companies have only one month from the date of receipt of a data subject access request to comply. If a request is received on 2nd October then you have until 2nd November to comply with the request. It is possible to seek an extension for a further two months if the request is particularly complex or there have been a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Organisations will need to have policies and procedures in place to set the criteria for refusal. When a refusal is made, employers will then need to be able to demonstrate why the request met that criteria. Subject access requests are generally quite complex and time-consuming to deal with as many requests can be vague or require extensive searches to be undertaken with various people across the organisation.

## MARKETING

Someone can only be contacted for marketing if they have given consent or if there is an existing relationship with them and a similar product or service is being offered. To prove consent has been given, some firms operate a double opt - in model.

After initial consent is given, an e-mail is sent to the individual asking them to click the link to validate that consent. It will be more difficult to justify automated targeting or profiling of people using their personal information. The reasons for making automated decisions about a person must be explained.

For example, targeting adverts for baby products at someone who searches for morning sickness may be unlawful profiling based on the collection of sensitive personal information.

## PENALTIES

Failure to comply with the GDPR can result in fines of up to 20 million Euros or 4 per cent of a company's (or the entire group company's) annual worldwide turnover so employers must not ignore this area.

# So what do we do now?

## GDPR CHECKLIST

| | |
|---|---|
| Think about a data audit and data register for your organisation. | ☐ |
| Review the ways you currently obtain consent and assess if these will be valid under the GDPR. If not, change your procedures. | ☐ |
| Consider what alternative conditions you can rely on for using personal data. | ☐ |
| Check if you collect any genetic or biometric information and implement procedures for protecting sensitive personal data. | ☐ |
| Make sure there is a procedure in place for acting on a request to withdraw consent. | ☐ |
| Make sure company policy on personal data will be updated in reference to the eight data protection principles. | ☐ |
| Consider privacy by design and privacy by default in new and existing applications. | ☐ |
| Ensure you have procedures for dealing with data subject access requests and right to be forgotten requests. | ☐ |
| Consider if you need to appoint a data protection officer in the organisation. | ☐ |
| Check and update your privacy notices. | ☐ |
| Review any current or future contracts with data processors. | ☐ |
| Think about setting up a central data breach management register. | ☐ |
| Consider how the GDPR may impact on any international data transfer. | ☐ |
| Ensure staff have adequate and regular training on data protection and the GDPR changes. | ☐ |

For further **expert legal advice**, please contact our employment specialist, Jane Crosby, directly.


**01483 887742**

**jzc@hartbrown.co.uk**


HART BROWN
SOLICITORS

**hartbrown.co.uk**