A&L Goodbody

GDPR for Employers

DUBLIN / BELFAST / LONDON / NEW YORK / SAN FRANCISCO / PALO ALTO

1 Consent

Things you need to know about consent and the processing of employees' data

The EU General Data Protection Regulation (GDPR) introduces substantial changes to data protection law which will impact the employer/employee relationship once it comes into force on the 25 May 2018. One area that will be impacted is reliance by the employer on the employee's consent to process their data. It is common practice for employment contracts to include a blanket consent provision under the heading "data protection". Typically this will provide that the employee consents to the use and processing of their data under the contract (e.g. transfer of data overseas, monitoring, disclosure of sensitive personal data to third parties and the sharing of information with a wide variety of partners for payroll, insurance and health related purposes). It is unlikely that this form of consent will be held to be effective once the GDPR comes into operation and even if it is, employees have a right to withdraw their consent at any time.

Reliance on consent post 25 May 2018

If you as an employer want to rely on consent as the basis on which to process an employees' data, the employees' consent should be separate from the contract or, if contained within the employment contract, it should be clearly distinguishable from other aspects of the document and a separate signature box is required. Employees will have a stronger right to have their data deleted where consent is relied on as a legal basis for processing. Prior to giving consent, employees must be told of their right to withdraw consent at any time and it must be easy for them to do so (i.e. allowing consent to be withdrawn in the same medium in which it was obtained, such as via a website or email). For these reasons an employer should look for an alternative legal basis for processing in the first instance so that if consent is withdrawn the employer is not prohibited from processing personal data.

Alternatives to consent can be considered in the following circumstances

1. Where the processing is necessary for the performance of the contract with the employer or to enter into such a contract.
2. Where the processing is necessary for compliance with a legal obligation to which the employer is subject.
3. Where the processing is necessary to protect the vital interests of the employee or another person.
4. Where the 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 employer.
5. Where the processing is necessary for the purposes of the legitimate interests of the employer or a third party except where such interests are overridden by the interests of the employee.

Some practical flexibility has been built in to the GDPR itself. For example, the GDPR acknowledges that the transmission of personal data within a group of undertakings for internal administrative purposes, including the processing of employee data constitutes a legitimate interest (point 5 above).

Sensitive Data and the need for explicit consent

Where consent is relied on as a ground for processing sensitive data the GDPR requires such consent to be explicit. That is not new. In practice this must mean that consent is clear, specific and unambiguous. Employee data is sensitive much of the time e.g. racial or ethnic origin, religious beliefs, trade union membership, data relating to health including mental health and sexual orientation. Again an employer should look for an alternative legal basis for processing in the first instance so that if explicit consent is withdrawn the employer is not prohibited from processing sensitive data.

Alternatives to consent can be considered in the following circumstances

- Where the processing is necessary for carrying out the legal rights and obligation of the employer and employee as authorised by employment/social protection law or contained in a collective agreement.
- Where the processing is necessary to protect the vital interests of the employee or another person where the employee is physically or legally incapable of giving consent.
- Where the processing is necessary for a not-for-profit organisation with a political, religious, philosophical or trade union aim, and the processing is solely for their members.
- Where the processing is related to data which has manifestly already been made public by the employee.
- Where the processing is necessary for the establishment or defence of a legal claim.
- Where the processing is necessary for substantial public interest reasons.
- Where the processing is necessary for the assessment of the working capacity of the employee.
- Where the processing is necessary for public health reasons.
- Where the processing is necessary for archiving purposes in the public interest, scientific, historical research or statistical purposes.

What happens if businesses don't comply?

Breaches of the new rules could result in an increase in employment disputes and employers could face maximum fines for data protection breaches of up to €20 million or 4% of global turnover.

2 Privacy Notices

Things you need to know about privacy notices

The GDPR widens the scope of mandatory information that must be provided to employees to ensure that the processing of their data is fair and transparent.

From 25 May 2018, employers will be required to provide employee and other data subjects, by way of a privacy notice, with the following information:

- The identity and contact details of the employer or its representative;
- The contact details of the data protection officer, where applicable;
- The purpose of the processing and the legal basis for the processing;
- The legitimate interests of the employer or a third party and an explanation of those interests (where processing is based on this ground);
- The recipients or categories of recipients of the personal data;
- Details of any transfers out of the EEA, safeguards in place and the means by which to obtain a copy of them.

Information required for fair and transparent processing

In addition to the above the employer is required, for the purposes of ensuring that the processing is fair and transparent, to provide the following information:

- The data retention period or criteria used to determine same;
- The employee's rights, including the right of access to data; rectification and erasure; restriction of the processing; objection to processing and to data portability;
- Where the processing is based on consent, the right to withdraw it at any time;
- The right to complain to the supervisory authority;
- Details of automated decision making, including profiling and logic involved, as well as the significance and consequences of such processing for the employee, and
- Whether the provision of personal data is a statutory or contractual requirement or obligation, and the consequences of failure to provide such data.

Data that the employer obtains directly from the employee

Where the employer obtains the employees' personal data directly from them, the privacy notice must be supplied at the time the personal data is obtained.

Data that the employer obtains indirectly from the employee

Where the employer does not obtain the data directly from the data subject, it must, within one month of obtaining the data, provide the employee with a similar privacy notice to that referred to above, and in addition, the categories of data processed; from which source the data originated; and, if applicable, whether it came from publicly accessible sources.

Further processing

Where the employer intends to further process the data other than for the purpose for which it was collected, the employer must inform the data subject, prior to the further processing, of that other purpose.

What happens if businesses don't comply

Breaches of the new rules could result in an increase in employment disputes and employers could face maximum fines for data protection breaches of up to €20 million or 4% of global turnover.

3 Data Subject Access Requests (DSARs)

Things you need to know about Data Subject Access Requests (DSARs)

From 25 May 2018 the time period for an employer to respond to a DSAR will be reduced from 40 days to one calendar month. This can be extended by a further two months where requests are complex or numerous. However, the employee must be informed of any proposed extension within one month of the employer's receipt of the DSAR. In practice, we anticipate many employers will seek to portray requests as complex and/or numerous to avail of the three month extension.

DSAR fee has been abolished

The ability to charge a fee has been removed. However an employer may charge a reasonable fee for any further copies requested or where access requests are clearly unfounded or excessive.

What information is the employer obliged to provide?

When providing employees with their data employers must provide the following information:

- The purpose of processing the data
- The categories of personal data
- The recipients or categories of recipients
- The data retention period or criteria used to determine the criteria
- The individual's rights including their right to correction, erasure; restriction or objection to the processing
- The right to complain to the Office of the Data Protection Commissioner
- The source of the information, if not collected directly from the data subject
- Details of any automated processes including profiling and the significance and envisaged consequences of the processing for the data subject
- Where data is transferred out of the EEA, the appropriate safeguards that are in place.

What is the deadline for compliance?

Employers have until the 25 May 2018 to make sure their processing practices meet with new regulations.

What happens if businesses don't comply?

Breaches of the new rules could result in an increase in employment disputes. Employers could face maximum fines for data protection breaches of up to €20 million or 4% of global turnover.

4 Security Obligations

Enhanced security measures

The EU General Data Protection Regulation (GDPR) increases employer obligations to protect the security and integrity of personal data. Data must be protected by *"appropriate technical and organisational measures"*.

In particular the employer should consider the risks presented by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

"Appropriate technical and organisational measures" are described as including:

- Pseudonymisation (replacing any identifiable characteristics of personal data with a pseudonym so that the data subject cannot be directly identified) and the encryption of data.
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, accessing and evaluating the effectiveness of technical and organisational measures to ensure the security of the processing.

Pseudonymisation

Pseudonymisation is a security measure which can be applied to data (e.g. a HR report), to make the employees impossible to identify without additional information which is stored separately from the data. What appears in the data report will depend on what information the employer/HR has been asked to provide e.g. below are details needed to calculate the cost of collective redundancies.

Security Measure	Number	Name	Job Title	Location	Service	Notice	Salary
None	1	Jane Doe	Operator	Dublin	5 years	3 months	40,000
Inadequate anonymisation	1		Operator	Dublin	5 years	3 months	40,000
Pseudonymisation	L0247				5 years	3 months	40,000

Action points

- Employers must demonstrate that they have complied with security obligations, by showing that they have followed an approved code of conduct or have an approved certification mechanism.
- Employers should stress test HR IT systems to ensure ability to back up and restore employee data and to protect it using firewalls and anti-virus security measures.
- Where possible, HR data should be made difficult to understand in the case of unauthorised access.
- The application of pseudonymisation and encryption for HR reports should become routine.
- Limit access to only those who need the data, using passwords and access permissions.
- Provide employee training and highlight the right to discipline employees for data protection breaches.

Data Breach Reporting within 72 hours

The GDPR introduces a new mandatory obligation requiring employers to notify data breaches to the Data Protection Commission (DPC) "*without undue delay, and where feasible, not later than 72 hours after having become aware of it*". If notification is not made after 72 hours, a reasoned justification for the delay must be provided.

The employer must keep a record of any data breaches, including its effects and the remedial action taken. This will enable the DPC's office to verify the controller's compliance with its breach notification obligations.

Employers must also notify data breaches to data subjects where the breach is likely to result in a "high risk" to the data subject. *"High risk"* could include data that could result in identity theft/fraud, financial loss, damage to reputation, loss of confidentiality of personal data, or release of sensitive data.

Action points

- Ensure the data breach response plan identifies the key personnel responsible for dealing with the breach and informing the supervisory authority/data subject.
- That the individual has adequate training to determine whether a report to DPC is required or not.
- Data processing agreements with third party providers e.g. payroll providers, should be reviewed to ensure that they include a requirement for the processor to immediately inform the employer of any data breaches.

5 The Final Countdown - HR To-Do List

What do I need to have in place for my employees?

Privacy Notice - the GDPR sets out a list of information which employers must provide to employees, in a clear and user friendly manner. We recommend that you have a separate Privacy Notice in place for job applicants as the information to be given to them will be different to the information to be given to employees. Read our Guide to Privacy Notices.

Data Protection Policy - the GDPR does not specify what information must be in a Data Protection Policy. Your policy can therefore be tailored to your business and should include key messages to employees e.g. we take data protection seriously, security rules must be followed when handling any data, breach of this Policy will lead to disciplinary action.

What do I need to do with contracts of employment?

Amend contracts to remove any reference to the consent of employees to data processing. Read our Guide to Consent. Also, introduce the concept of disciplinary action for data protection breaches.

Remember that contracts already in place with current employees may only be amended with the consent of each individual employee. We recommend that you leave these contracts in place as they are, issue a Privacy Notice and explain to employees that you no longer rely on the consent provisions in their contracts.

What about the third parties who look after payroll, recruitment, benefits, pension etc?

Amend contracts which govern these arrangements – the GDPR sets out a list of terms which must be imposed by you on the third party who is processing employee data, on your behalf.

Anything else?

If you haven't already done so, complete your audit to establish what employee data you hold, for how long, for what reason, and the legal basis.

Sample HR Audit Report (extract only)

Business Functions	Purpose of Processing	Category of Individual	Category of Personal Data	Legal Basis	Retention Period	Location
Finance	Payroll	Employee	Income Tax	Article 6 (1) c - Legal Obligation	11 years	Payroll system
HR	Personnel	Employee	Annual Leave Details	Article 6 (1) b - Contract	3 years	HR personnel system
HR	Recruitment	Job Applicant	Qualifications	Article 6 (1) b - Contract	12 months	HR recruitment system

Action points

1. Identify and document what basis you have for processing employee data, as the consent of your employees is no longer a recommended option. Read our Guide to Consent.
2. Audit your employee data. Know what you hold and why.
3. Put a retention policy in place. Take advice so you know what you are obliged to hold by law (e.g. employment contracts, employment permits, records of working time, annual leave, redundancy calculations) and for how long.
4. Draft and issue your Privacy Notice to employees – make sure it covers all of the mandatory points set out in the GDPR. Read our Guide to Privacy Notices.
5. Draft and publish your Data Protection Policy – make sure it is tailored to your requirements and what you expect from your employees in terms of employees' obligations to protect data.
6. Amend your employment contract template to remove any reference to consent to data processing. Read our Guide to Consent.
7. Tell employees that you are no longer relying on the data protection consent clause in their contracts. Communicate this in writing.
8. Review your security measures for keeping employee data safe. Read our Guide to Security.
9. Amend HR related third party contracts. Make sure they cover all of the mandatory points set out in the GDPR.
10. Consider training employees – this will help you to demonstrate your commitment to compliance with the GDPR and avoid mistakes being made by your employees.

6 Key employment documents

1. HR Data Audit Report
2. Privacy Notice
3. Data Protection Policy
4. Contract of employment
5. Communication to employees
6. Contracts with HR related third parties/service

How we can help

- Employee data audit
- Draft employee Privacy Notices
- Update employee contracts
- Advice on Data Protection Policy
- Advice on retention periods
- Employee communication - consent and new approach to data processing
- Update third party contracts
- Tailored consent provisions - e.g. processing of sensitive personal data
- Advice on data transfer
- Data Subject Access Request (DSAR) advice
- HR data breach management
- Employee training

OUR TEAM

Duncan Inverarity
Partner
+353 1 649 2401
dinverarity@algoodbody.com

Ciara McLoughlin
Partner
+353 1 649 2321
cmcloughlin@algoodbody.com

Gareth Walls
Partner
+44 28 9072 7402
gwalls@algoodbody.com

Ailbhe Dennehy
Associate
+353 1 649 2431
adennehy@algoodbody.com

Rachael Evans
Associate
+353 1 649 2784
revans@algoodbody.com

Aisling Muldowney
Associate
+353 1 649 2577
amuldowney@algoodbody.com

Maria Pittock
Associate
+353 1 649 2651
mpittock@algoodbody.com

Kevin Slattery
Solicitor
+353 1 649 2217
kslattery@algoodbody.com

Karen Killalea
Partner
+353 1 649 2118
kkillalea@algoodbody.com

Ian Moore
Consultant
+353 1 649 2412
imoore@algoodbody.com

Michael Doyle
Associate
+353 1 649 2729
mvdoyle@algoodbody.com

Ciaran Ahern
Associate
+353 1 649 2933
cahern@algoodbody.com

Noeleen Meehan
Associate
+353 1 649 2206
nmeehan@algoodbody.com

Brid NicSuibhne
Associate
+353 1 649 2274
bnicsuibhne@algoodbody.com

Audrey Whyte
Solicitor
+353 1 649 2101
awhyte@algoodbody.com

Denise Moran
Solicitor
+353 1 649 2663
dmoran@algoodbody.com


CONNECTED
CHECKING
02 12.123.8234
CONNECTED
CHECKING
[PROCESSING]