General Data Protection Regulation (GDPR)

GDPR Policy Document

Relating to:

Avantus Business Solutions Limited and its subsidiaries:

- **Fair Care Employee Benefits limited**
- **Avantus Systems Limited**
- **People Care Human Resources Limited (inc. Avantus Recruit)**

Index:

Last updated: 02/01/2018

Introduction

The GDPR applies in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Avantus Business Solutions Limited and its subsidiary companies ('the group') will need to be fully compliant ahead of May 2018.

Different elements of the group act in different capacities. As an employer and a recruiter, we act as a Data Controller; in our Flexible Benefits and HR systems businesses (both direct and enterprise versions), we act as a Data Processor.

The GDPR makes Data Processors directly accountable to the Information Commissioner and in consequence, Data Processors can be fined directly by the ICO. This is a key change from the former DPA regulations.

10 Steps to Getting Ready

There are 10 key activities in process that will prepare us for GDPR:

1 Awareness & Training – All staff need to appreciate the impact of GDPR. This GDPR Policy Document is available to all staff. Where staff process personal data, further training is being given and GDPR online course need to be completed and passed.

2 Information Analysis – We are documenting the personal data we hold, where it comes from and who we share it with.

3 Privacy Notices – We are updating our privacy policies in line with GDPR (adding lawful basis for processing data, retention periods etc) and considering changes to how the policies appear when users access our products.

4 Individuals' Rights – We are checking procedures to ensure we meet the requirements of GDPR. There is detailed guidance on how information should be managed.

5 Subject Access Requests – We are updating our processes/systems so that we can quickly and easily produce all personal data in respect of an individual (data subject).

6 Lawful Basis for processing personal data – we are assuming that we can rely on a lawful basis to process personal data (both as an employer and a Data Processor for our clients) as opposed to gaining consent. The GDPR includes lawful bases: 'where processing is necessary for the purposes of legitimate interests pursued by the Controller or third party; except where such interests are overridden by the interests, right or freedoms of the data subject.' Or 'for the performance of a contract with the data subject or to take steps to enter into a contract'.

7 Consent – we will not need to rely on consent from data subjects if the Lawful Basis is accepted. We are seeking legal opinion on this.

8 Data breaches – We are reviewing/updating existing policies to ensure we have appropriate documented processes to detect, report and investigate a personal data breach.

9 Data Privacy Impact Assessment – we are considering if we need to implement an assessment process based on ICO code of practice ahead of May 2018

10 Contractual Concerns – we are currently reviewing our contracts with employees and clients to assess if we need to make any contractual changes, or/and statements of clarification defining which role we are undertaking and where any liability may lie.

Background to GDPR – Key Elements:

A Data Processor must maintain records of personal data and processing activities.

A Data Controller is obliged to ensure contracts with Data Processors comply with GDPR.

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Article 5 of the GDPR further requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data. You can, however, rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

GDPR - Individuals' Rights

1. The Right to be Informed

In brief - the right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

2. The Right of Access

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can we charge a fee for dealing with a subject access request?

You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

3. The Right to Rectification

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

In more detail…

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

4. The Right to Erasure

In brief…The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

In more detail…

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

5. The Right to Restrict processing

In brief…Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

In more detail…

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

6. The Right to Data Portability

In brief…The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

7. The Right to Object

In brief…**When does the right to object apply?**

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and

- processing for purposes of scientific/historical research and statistics.

In more detail…

How do I comply with the right to object?

If you process personal data for the performance of a legal task or your organisation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If you process personal data for direct marketing purposes

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

These requirements are similar to existing rules under the DPA.

If you process personal data for research purposes

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

If your processing activities fall into any of the above categories and are carried out online:

You must offer a way for individuals to object online.

8. The Right Related to Automated Decision Making

In brief…

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

In more detail…

When does the right apply?

Individuals have the right *not to be subject to a decision* when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

What else does the GDPR say about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

You must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) **must not**:

- concern a child; or
- be based on the processing of special categories of data unless:
- you have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Accountability and Governance

What is the accountability principle?

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing; and
- Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

You can also:

- Adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.

Records of processing activities (documentation)

As well as your obligation to provide comprehensive, clear and transparent privacy policies (see section on Individual rights), if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

• processing personal data that could result in a risk to the rights and freedoms of individual; or
• processing of special categories of data or criminal convictions and offences.

What do I need to record?

You must maintain internal records of processing activities. You must record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).

- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Data protection by design and by default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Under the DPA, privacy by design has always been an implicit requirement of the principles - eg relevance and non-excessiveness - that the ICO has consistently championed. The ICO has published guidance in this area.

Further reading in the GDPR

- See Article 25 and Recital 78
External link

Data protection impact assessments

What is a data protection impact assessment?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach. See the ICO's Conducting privacy impact assessments code of practice for good practice advice.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

  This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.
- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Breach Notification In more detail…

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Example

A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

What breaches do I need to notify the relevant supervisory authority about?

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

What should I do to prepare for breach reporting?

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data.
You should ensure that you have an internal breach reporting procedure is in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Transfer of Data

- In brief…**The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.**

National Derogrations

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.