Advantage
transform the way you work

ADVANTAGE INSIGHTS

# GDPR

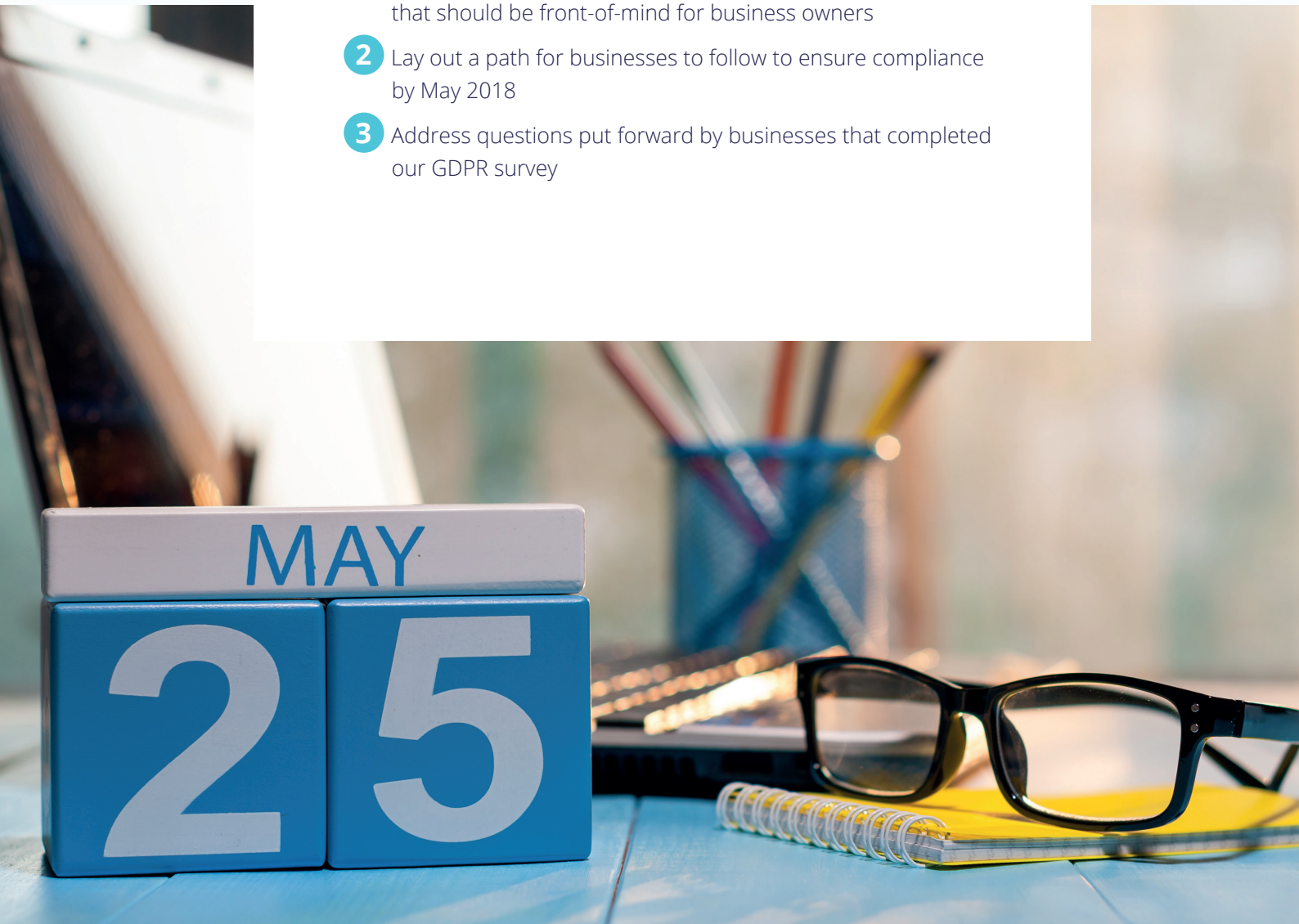
## GENERAL DATA PROTECTION REGULATION

# INTRODUCTION

On 25 May 2018, the EU's General Data Protection Regulation (GDPR) will come into effect and apply to all businesses – regardless of size - operating in the U.K., as well as all businesses outside the EU that collect or process the data of EU citizens and residents.

**The purpose of this document is threefold:**

1. Introduce the GDPR and highlight key pieces of the legislation that should be front-of-mind for business owners
2. Lay out a path for businesses to follow to ensure compliance by May 2018
3. Address questions put forward by businesses that completed our GDPR survey



# THE GDPR – WHAT I NEED TO KNOW?

The **GDPR** is a legal framework intended to further secure individuals' personal data from businesses, organisations and institutions. The legislation puts in place strict guidelines as to how a person's information can be collected, used and stored, as well as making clear the rights individuals have when it comes to their data.

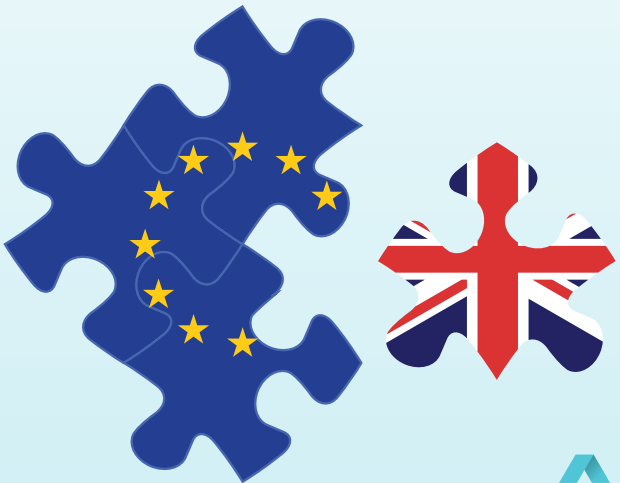
Even though data protection legislation is nothing new – all U.K. businesses currently comply with the Data Protection Act 1998 (DPA) – the purpose of the **GDPR** is to better align the rights of individuals and their data with the advances in technology that have taken place over the last 20 years. Make no mistake about it, the **GDPR** will dramatically change the way your business operates, and every single business function (not just IT) will need to adhere to these changes. However, in a world where all your information is stored online it's good to know that there are protections being put in place that ensure your private and personal information are safe.

# THE GDPR & BREXIT

The U.K.'s withdrawal from the European Union has absolutely no bearing on the **GDPR**. Whether inside or outside of the EU, if your business or organisation collects or processes the information of EU citizens and residents, you are required to comply with the **GDPR**: *failure to do so will result in severe fines and reputational loss.*

Organisations that send their customers' information outside of Europe for processing – for example, to the Americas or Asia – should take note of informing their overseas partners of the **GDPR**. It will apply as equally to them as it will to any other business that works with EU citizens' and residents' data.

For the U.K. in particular, it's important that businesses make compliance to the **GDPR** their number one priority as the U.K. government has confirmed it will bring the **GDPR** into U.K. law under a new Data Protection Bill, ensuring its legal application to British citizens post Brexit.



# CONTROLLERS & PROCESSORS

## Controller

An organisation that determines the purpose, conditions and means for processing personal data is known as a controller. They are the initial collectors of the data.

## Processor

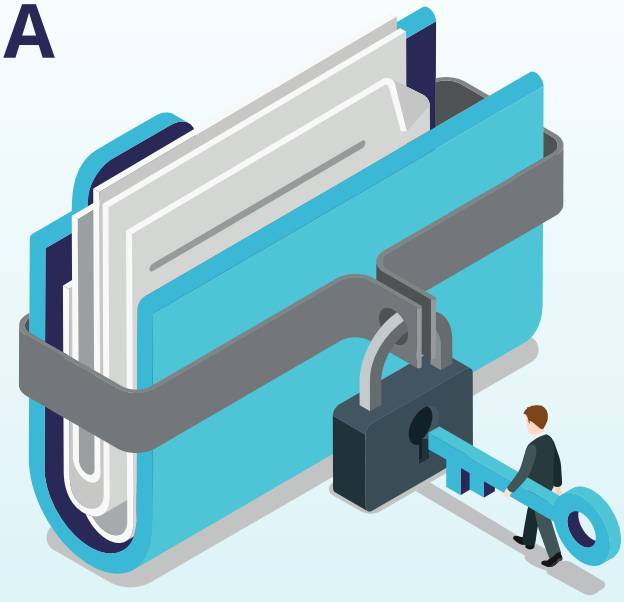
An organisation that processes data on behalf of their customer (the controller) is known as a processor.

**Both Controllers and Processors are individually responsible for complying with the GDPR.**

# PERSONAL DATA

As businesses and organisations increasingly digitise every aspect of their interactions with customers and employees, the definition of 'personal data' has expanded under the GDPR to include new digital identifiers that were previously not covered under the DPA. As stated in the Official Journal of the European Union, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

This expanded definition of 'personal data' will have significant implications for both controllers and processors. As the above states, any single unit of information or combination of units of information that can be used to identify an individual will be considered 'personal data' under the GDPR. This will include information such as political opinions, religious or ideological beliefs, genetic/biometric data and sexual orientation that can be combined with any other information, such as an IP address, to identify a person. Making sure your business is aware of all the data it holds, regardless of how generic you might think it is, is absolutely crucial to ensure your firm's compliance.



**And remember, your employees – including any information you might have on their family, such as a next of kin – all fall under the GDPR as well.**

# THE INDIVIDUALS' RIGHTS

Under the GDPR, individuals have a far greater say as to how their personal information is used by companies, organisations and firms. Comprising of the following eight rights, these are collectively known under the legislation as **'the individuals' rights,'** they are:

## The right to be informed

1

Under the GDPR, an organisation is obliged to explicitly inform an individual when their data is being processed in an intelligible and easy to understand manner; written in clear and plain language and appropriate to the individual's age group (for example, when they're collecting data off children they must use language an average child of that age would easily understand).

More importantly, individuals need to be made aware of the types of data being collected on them, how that data will be used and for how long, as well as how they can go about removing their consent if at some point in the future they decide they no longer want their personal information stored by that organisation.

2

## The right of access

In order to ensure transparency, the GDPR provides guidelines on how an individual can go about accessing all the personal data an organisation might hold on them. In essence, individuals have a right to know what personal data of theirs is being processed and they should also be able to access that data.

For those organisations that are currently complying with the DPA, one of the biggest differences this right brings forth is the removal of the £10 subject access fee. Organisations must provide individuals with a copy of their information for free, unless an organisation is able to justify that said individual's request is unfounded or excessive. Again, however, the individual needs to be informed as to why their request is unreasonable and the matter can result in an escalation to the Information Commissioner's Office (ICO).

Once a request has been made, organisations have one month to respond to the individual.

## The right to rectification

3


If an individual wishes to update their personal information or upon receipt of some communication notices their details are incorrect, they have a right to have that information rectified. It is the responsibility of the organisation to ensure that any third-parties that are privy to said information are updated of the changes, i.e. processors.

Rectification requests need to be responded to within one month, however, if the request is sufficiently complex it can be extended to two.

# The right to erasure, aka, ‘the right to be forgotten’

4

Individuals who feel an organisation no longer has a valid or lawful reason for processing their data can request that their information be removed and deleted.

**It is important to note that the right to erasure does not always apply and an organisation can refuse to comply with a request when:**

- Personal data is processed in order to exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- The exercise or defence of legal claims

**Organisations have to comply with ‘the right to be forgotten’ when:**

- 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
- 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, i.e. online services, to a child

5

# The right to restrict processing

**If an individual wishes to halt the processing of their personal data they are entitled to do so when the following conditions are relevant:**

- An individual contests the accuracy of the personal data; information should not be processed until its accuracy has been verified
- When an individual has objected to the processing of their personal data and you are in the process of reviewing if your organisation has legitimate grounds to override the individual’s request
- When processing is unlawful and the individual opposes erasure and requests restriction instead
- If an organisation no longer needs the personal data but the individual requires it in order to establish, exercise or defend a legal claim

# The right to data portability

6

The right to data portability allows individuals to move, copy or transfer their personal data with ease from one IT environment to another, i.e. from one organisation to another. This transfer should be done in a safe and easy manner and organisations are required to provide the individual with their data in a commonly used, machine readable form, such as a CSV file.

The information must be provided to the individual at no cost and organisations have a one month response time, unless the request is sufficiently complex, in which case it can be extended to two.


7

# The right to object

**An individual has the right to object to their data being processed when:**

- Their objection is based on legitimate interests or the performance of a task is in the public interest/exercise of official authority (including profiling)
- It will be used for direct marketing
- Processing for purposes of scientific/historical research and statistics

**An organisation can refuse an individual's objection only on the following two grounds:**

- When 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

# Rights related to automated decision making and profiling

8

The GDPR ensures individuals have a right to not be subject to a decision when it is based on automated processing and produces a legal effect that could cause a significant impact on the individual.

As with all of the GDPR's 'Individuals' rights' there are exceptions, and these are grounded on the legitimacy of the need to have automated decisions. For example, the right does not apply if the decision is: necessary for entering into or performance of a contract between an organisation and the individual, it is authorised by law, or it is based on explicit consent.

In regards to profiling – that is, when an organisation evaluates certain personal characteristics of an individual, such as their health, behaviour, movements, performance at work etc. - an organisation must make sure appropriate safeguards are in place. Safeguards include, ensuring processing is fair and transparent, uses appropriate mathematical or statistical procedures and implements appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

# Your responsibilities as an organisation

As the 'individuals' rights' show, the GDPR places a tremendous amount of responsibility on organisations, and the burden of this responsibility cannot and should not be shouldered by an organisation's IT department alone. The GDPR is not solely about finding the right technological solutions, but rather about ensuring organisations have proper processes in place, across all departments and employees, that promote the safe and lawful handling of individuals' personal information.

**Whereas previously the burden of proof was on the regulator to show an organisation was not being compliant, with the GDPR the burden of proof is on the organisation to show they are;** this shifts organisations' data protection strategy from a defensive position to an offensive one. If you do not take the time now to develop clear and compliant processes, technology alone will not be able to help you navigate the GDPR and your organisation will be found liable.

*This section will focus on making clear your responsibilities (in addition to those put forward in the 'individuals' rights') as an organisation under the GDPR. It will then provide a recommended blueprint for your organisation to follow in regards to developing a clear and compliant process.*

## Collecting, processing and storing data

One of the intended purposes of the GDPR is to restore trust between organisations and their stakeholders. The way this is done is by making clear the conditions under which an organisation is allowed to collect, process and store an individual's personal data. To that end, Article 5 of the GDPR states the following:

**"Personal data shall be:**

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

(b) Collected for specific, 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 of 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

Article 5(2) requires that, 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'"

Knowing and formalising your organisation's lawful basis for processing personal data is critical to your GDPR success as it will inform the extent to which the individual's rights apply in certain situations. In order for processing to be lawful it must first, explicitly have the individual's consent and second, the data must be needed in order to comply with a contract, a legal obligation, the data is in the public interest or if doing so is essential for the security and well-being of the individual and /or the controller has a legitimate interest.

### Defining consent under the GDPR

Central to the establishing of trust between an organisation and its stakeholders is the notion of consent. Whereas currently it is not uncommon for an individual to surprisingly find themselves on a mailing list or as the recipient of marketing communications from an unknown entity, under the GDPR this scenario will no longer be allowed. Come May 25, 2018, the days of assumed consent and pre-ticked boxes will be over.

Consent will need to be freely given, active and require an individual to opt-in, rather than out, to each individual way their data might potentially be used. As the ICO recommends, organisations need to make sure consent is "specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn."

**When it comes to children, the GDPR requires your organisation to have privacy notices written in clear, easy-to-understand and age appropriate language. If your organisation offers 'information society services' you will also need to obtain consent from a parent or guardian in order to process that child's data.**

# A CLEAR & COMPLIANT PROCESS

Hopefully you've realised by now that the GDPR is an ongoing journey, with 25 May 2018 being a start date, not an end. This complex piece of legislation will require time, vigilance and education, and your responsibility as a British business is to make sure you have everything in place today so you can avoid any potential risks post May 2018.

To ensure your business is GDPR ready, we recommend you take the following steps as soon as possible; with only a few months to go before the GDPR takes effect, ensuring your business has the right processes in place has to be your number one priority.

## 1 Communicate & Educate

Before you begin changing or implementing anything in regards to the GDPR, you should first make sure every single person in your organisation has been briefed on what the GDPR is and how it will affect their role. For those employees that deal directly with external data, such as marketing and human resources, additional educational sessions should be held. Every person working in your company – from the very top to the very bottom – should have a sound understanding of the GDPR and how it relates to the performance of their job.

A good way to make sure people understand these changes is to produce 'before and after' process maps. For example, whereas before you might have saved information directly onto your desktop, it is now company policy to save all documents in a designated shared server.

Once you've finished implementing your GDPR framework, it's a good idea to go back and do a refresh session with all employees, especially if you've introduced new technology to better manage the data you hold.

## 2 Discover

An obvious yet vital step on your journey towards GDPR compliance is to conduct an information audit in which you identify any and all personal data your organisation holds. Remember, this includes offline information that's on paper and in filing cabinets, as well as that which is stored digitally. As the GDPR also requires you to maintain a record of your data processing activities, we recommend you develop a data map alongside your information audit so you can see the movement of information in your organisation.

For example, once you've collected an individual's personal data what happens next? Do you send it externally for processing; do you use the same information, say an ID or reference number across multiple documents or forms?

Having a personal data workflow map will not only help you to discover what personal information you hold and where it's located, it will also help you identify whether you need to appoint a Data Protection Officer, in cases where the data processing volume is significantly large.

# 3 Manage

As mentioned earlier, under the GDPR, the burden of proof lies with the organisation and not the regulator, this means you are required to have a system in place whereby your organisation is able to clearly show it is complying with the data protection principles; the only way to do this is by having a clear data management process in place.

A data management process also allows you to quickly action any stakeholder requests that come as a result of the 'individuals' rights', for example, when an individual requests you remove or update their personal information, not only do you know exactly what information you have on said individual, you also know exactly where it is and you've put in place a process whereby that request can be actioned as quickly as possible.

By managing your data effectively, you are able to manage risk and control who has access to what. Go confidently about your business knowing you can easily demonstrate your compliance at any point.

Once you've gone through the discover and manage stages its important you develop internal (employees) and external (customers) communication plans so that all your stakeholders are aware of how your organisation uses and handles their personal data. This includes making sure your privacy statements – on all online and offline media – are up-to-date, clearly visible and written in easy-to-understand, plain, age appropriate language.

**Don't forget to include:**

- A detailed explanation of how an individual's data will be used, along with any third-party entities that might have access to the data
- Explicitly outline your lawful basis for processing the data
- Inform the individual how long you expect to hold and use their data for, and;
- How they can go about removing consent, updating their details or submitting a complaint
- Most importantly, don't forget to obtain active, opt-in consent

# 4 Protect

Cyber threats are here to stay and it's your responsibility as a data collector or processor to ensure you have put meaningful mechanisms in place to build up your security and prevent the personal data you hold from being compromised. With major cyber-attacks like Equifax, TalkTalk, T-Mobile, the NHS and many others taking place just within the last year, having inadequate security measures might be the easiest way for your business to be exposed and fined for not being GDPR complaint.

So important is security under the GDPR that the legislation makes 'data protection by design' a legal requirement, meaning, if your organisation is attacked and you are unable to prove you did everything within your power to prevent said attack, you will be fined €20 million or four percent of your global annual revenue (whichever is greater). This fine, along with the reputational damage and disheartened customers that come with a cyber-attack are enough to severely cripple even the biggest of organisations; if you're an SME it could spell the end of your business entirely.

Another security requirement that is mandatory under the GDPR is the 'Data Protection Impact Assessment', aka DPIAs. Your organisation will need to conduct a DPIA whenever a new initiative is likely to put an individual's personal data at risk. If for instance, you are deploying a new technology or introducing a new profiling operation, or you are processing data on a large scale, a DPIA will need to be conducted. If the DPIA shows there is a significant risk and you are unable to adequately address that risk, you will need to consult with the ICO and they will assess whether the processing complies with the GDPR.

**Start thinking about the initiatives your organisation has on the horizon that might require you to conduct a DPIA. It's important you know who will conduct them, who needs to be involved and how the process will be run.**

# 5 Report

While the GDPR is a much-needed law, it will inevitably expose your business to additional scrutiny, in the eyes of your detractors (internal and external), the GDPR will be seen as an opportunity to hurt your business. A detailed, systematic and consistent approach to reporting on your business' documentation practices, data management principles, how you process 'individuals' rights' requests, and how you respond to breach notifications are the only ways you will be able to defend yourself against any accusations of wrongdoing. Nothing could be more chagrin than being fined for something you know your business had no part in but due to a lack of stringent reporting you were unable to exonerate yourself.


# TRANSFORM THE WAY YOU WORK

As one of a select few Microsoft Partners in the U.K. to offer ERP, CRM and Managed Services to clients, Advantage is well positioned to provide your business with a holistic approach to GDPR compliance.

We understand that every business is unique and there is no one-size fits all approach to achieving compliance, that's why we start from a position of openness and learning. By actively listening, learning and ultimately understanding your business as a whole we are able to offer you solutions across the IT spectrum that deal directly with the nuances of your organisation.

**For each of the five process steps (Communicate and Educate, Discover, Manage, Protect, Report) we have a wide range of ERP, CRM and Managed Services solutions to support your GDPR compliance.**

Talk to Advantage today and start your GDPR journey the right way.

**0203 004 4600**

**hello@advantage.co.uk**

**ACKNOWLEDGEMENTS:**

Author: Camilo Lascano Tribin

Design by: www.csone.co.uk

Contributors and Reviewers: Richard Goddard, Mark Howe, Steve Godfrey, Jason Tucker.

**SOURCES:**

ICO's Overview of the General Data Protection Regulation (GDPR)

Official Journal of the European Union, Regulations (EU) 2016/679 of the European Parliament and of the council of 27 April 2016.

Advantage
transform the way you work

0203 004 4600 | HELLO@ADVANTAGE.CO.UK | WWW.ADVANTAGE.CO.UK