G.D.P.R

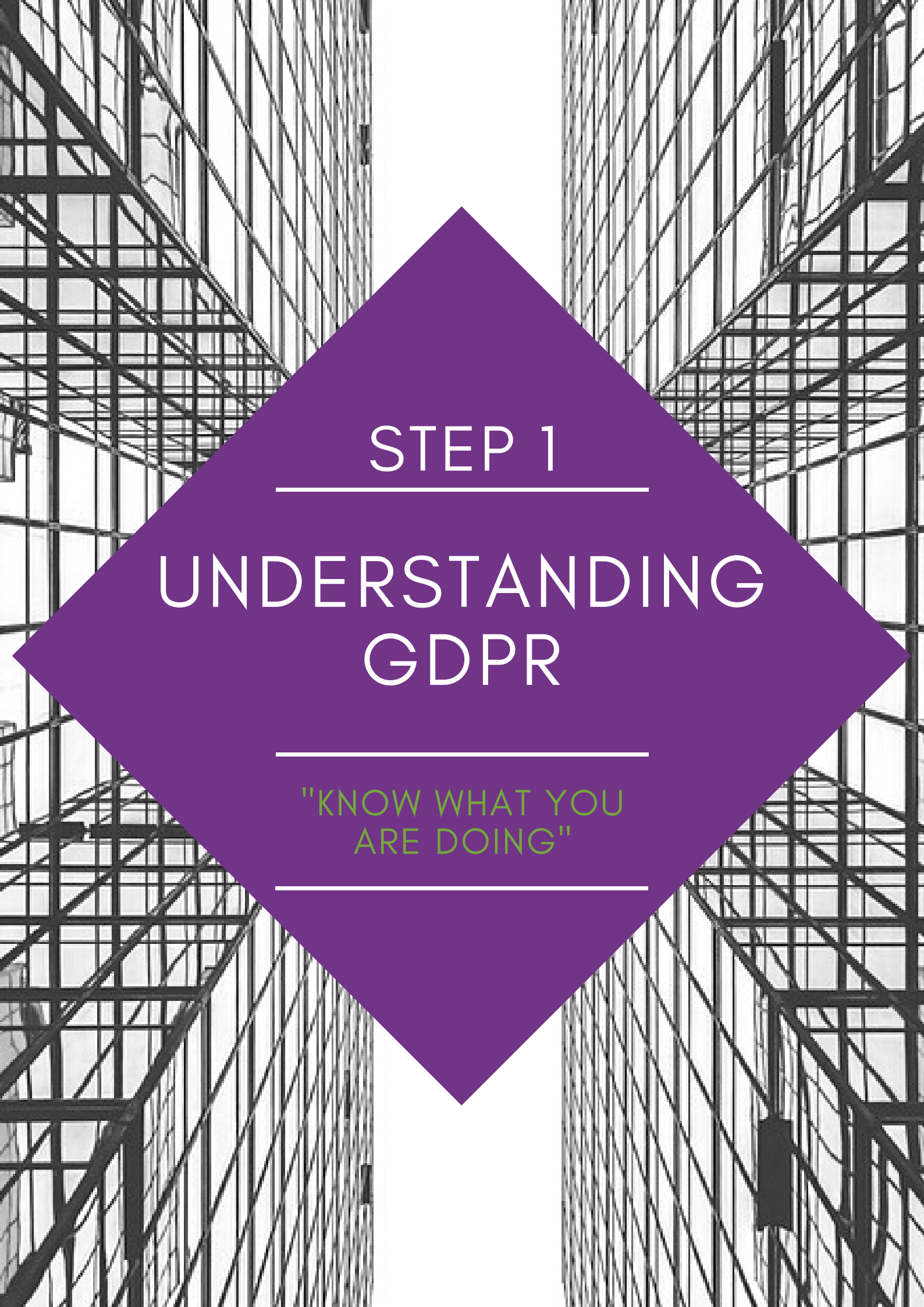
Made Easy

Hop on board as your GDPR journey starts here...

the business train
your journey starts here

THE

Table of Contents



STEP 1

UNDERSTANDING GDPR

"KNOW WHAT YOU ARE DOING"

WELCOME TO YOUR GDPR JOURNEY...

My name is Alan Hecht, Managing Director of The Business Train and we specialise in helping business owners become G.D.P.R compliant. This doesn't have to be an overwhelming journey and instead it can be a simple and easy process.

But before we start, let's just make sure you are at the right station:

Are you a business owner?
Have you registered with the ICO?
Do you use CCTV at your business?
Do you process any personal information on staff or clients?
Are you concerned that you may not be GDPR compliant?

Do you want a simple and fast way to be fully GDPR compliant?

If you answered YES to any of the above, then I would like the opportunity to share something very interesting with you that could change the course of your GDPR compliance journey. It's to get on the GDPR train.

It's not as complicated as you may think. Here at the The Business Train, we eliminate the stress and headaches that can come with doing it yourself, and you'll eliminate the huge price tag. We've calculated you can save over 90% compared to the cost of a lawyer or consultant. In other words, you'll save thousands of pounds and achieve the same end desired result - a complete set of GDPR policies providing you with the peace of mind that in the case of a data breach - the ICO will work with you rather than against you.

We live in a data-driven world which means you can't ignore the data your business stores. Almost every transaction and interaction you have with your clients or other businesses involves you sharing personal data. Starting with something as simple as your staff or clients name, address, date of birth and moving onto the data you share online.

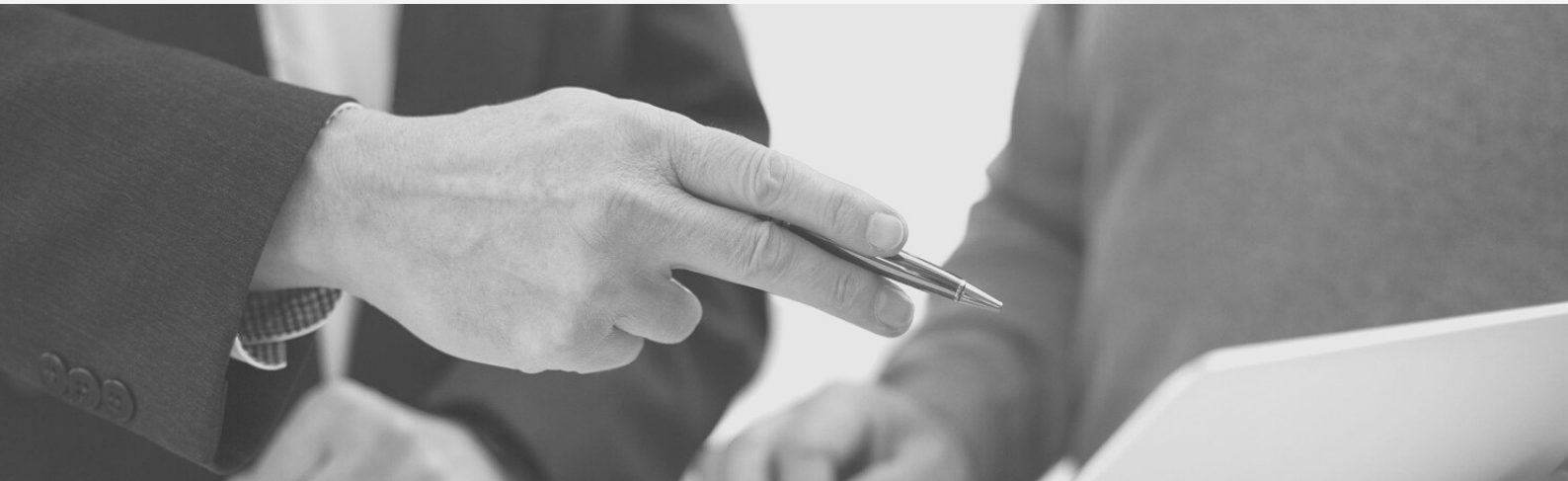
Every time you visit a website, search for or buy something, use social media or send an email, you are sharing data that helps to make life easier, more convenient and keeps everyone connected. But your data is your data and it belongs to you, so you need to make sure it is used properly, legally and it stays safe.

This is why the UK has set up its own independent body called the Information Commissioner's Office (ICO), to uphold your information rights. To increase the confidence you have in organisations that process your personal data and those which are responsible for making your information available to the public. The ICO requires every business that processes personal information to pay a registration fee, unless they are exempt.

Failure to do so will result in a fixed penalty. If you do not take yourdata protection responsibilitiesseriously, the ICO may alsotake enforcement action..

In the most serious cases of a breach, they can serve a monetary penalty of up €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

By following the advice of the ICO you will mitigate the risk of being fined if you are unfortunate enough to suffer a data breach.



THE ICO WEBSITE IS A USEFUL TOOL...

as a reference site but can sometimes be overwhelming with all of its legal content. Therefore we have created this simple to follow guide for you to quickly start your journey to learning what it all means for you and what you need to do next.

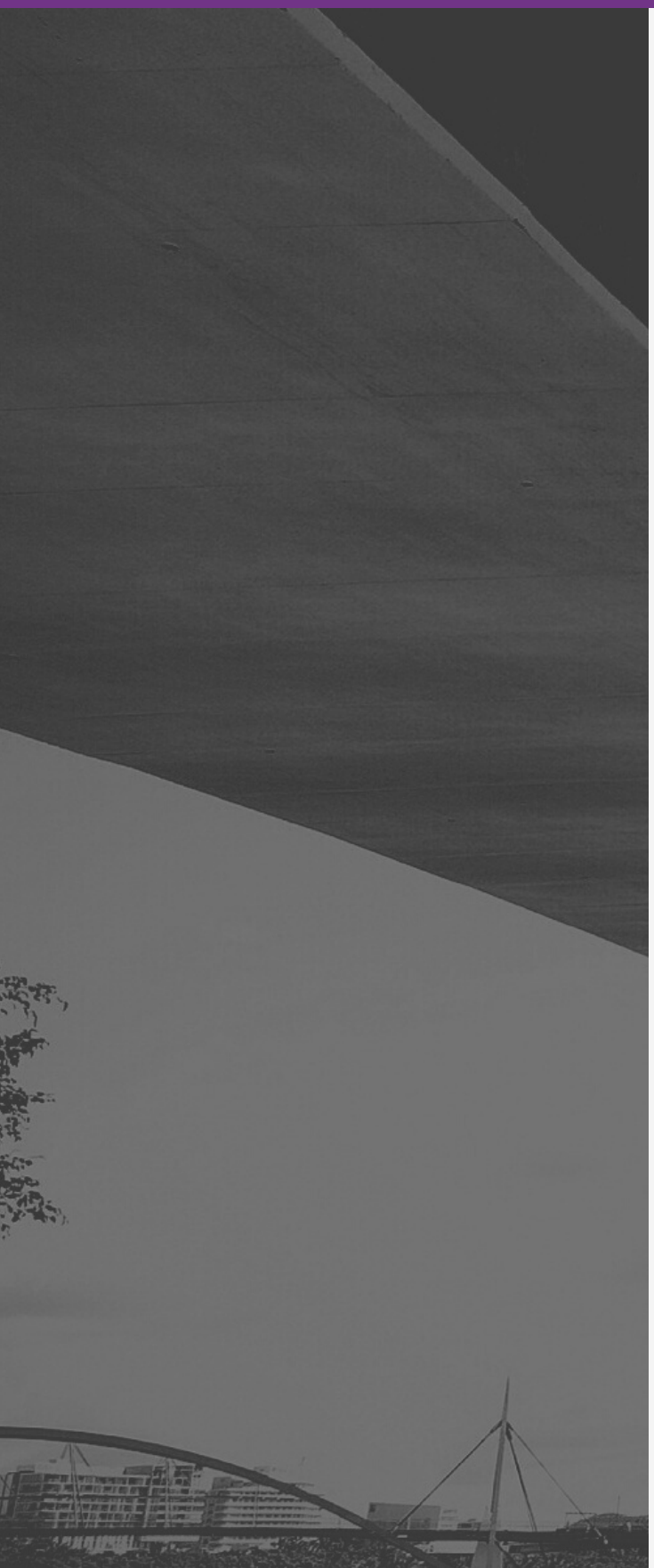
So let's jump on board the business train and start your GDPR journey. (on time)

Let's start with gaining a deeper understanding of General Data Protection Regulation (GDPR) and why it's focus is data protection.

DATA PROTECTION

Is the fair and proper use of information about people. It's part of the fundamental right to privacy, but on a more practical level, it's really about building trust between people and organisations.

HUGE STEP FORWARD

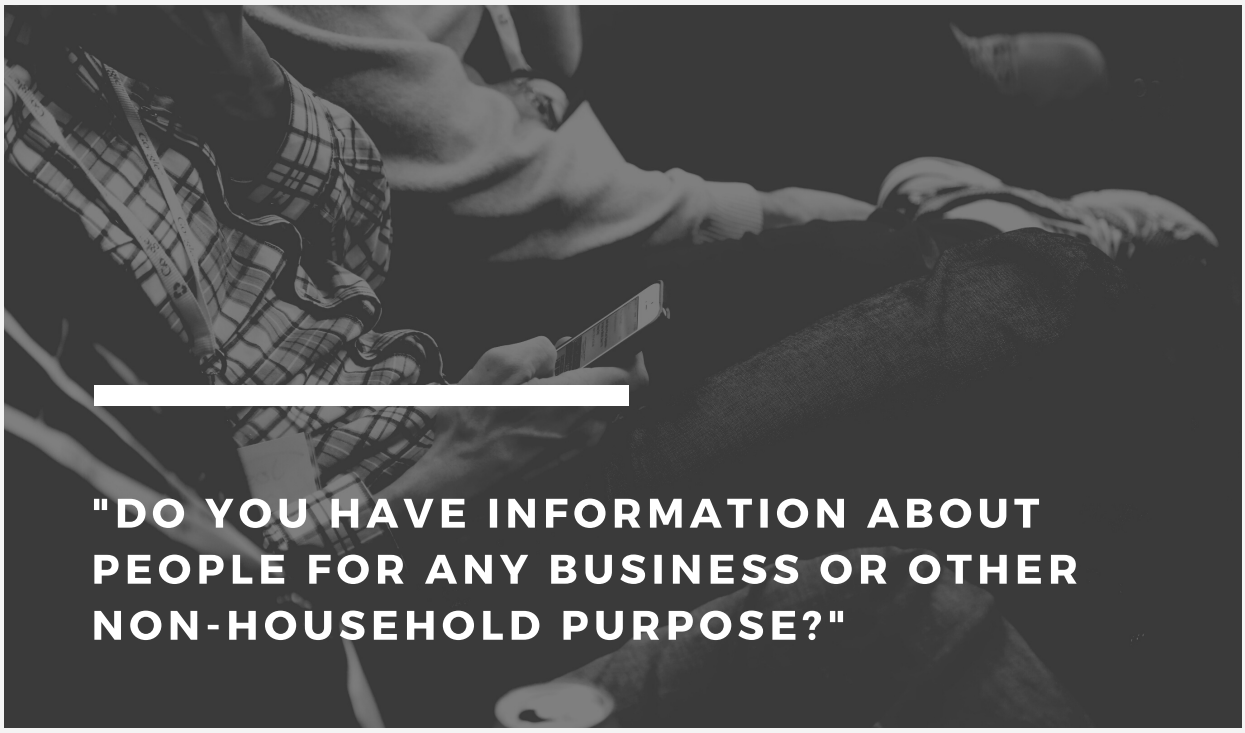


It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

It's also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders. The UK has been actively involved in developing these standards.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

INFORMATION ABOUT **PEOPLE**



The law applies to any 'processing of personal data', and will apply to most businesses and organisations, whatever their size.

You will not need to comply if you only use the information for your own personal, family or household purposes.

e.g Personal social media activity, private letters and emails, or use of your own household gadgets.

In short, personal data means information about a particular living individual.

PERSONAL DATA

"IT DOESN'T NEED TO BE 'PRIVATE' INFORMATION – EVEN INFORMATION WHICH IS PUBLIC KNOWLEDGE OR IS ABOUT SOMEONE'S PROFESSIONAL LIFE CAN BE PERSONAL DATA."

This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.

It doesn't cover truly anonymous information, but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

It only includes paper records if you plan to put them on a computer (or other digital device) or file them in an organised way.

THE ICO OFFER...

Advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

They also cooperate with data protection authorities in other countries. They are currently a member of the European Data Protection Board (EDPB), which includes representatives from data protection authorities in each EU member state, and they contribute to EDPB guidelines and other joint activities.

This guidance is designed to help small to medium-sized UK businesses and organisations keep personal data flowing with Europe (the EEA) after Brexit. (The EEA is the EU plus Iceland, Norway and Liechtenstein.)

The UK is committed to maintaining the high standards of the GDPR (General Data Protection Regulation) and the government plans to incorporate it into UK law after Brexit.

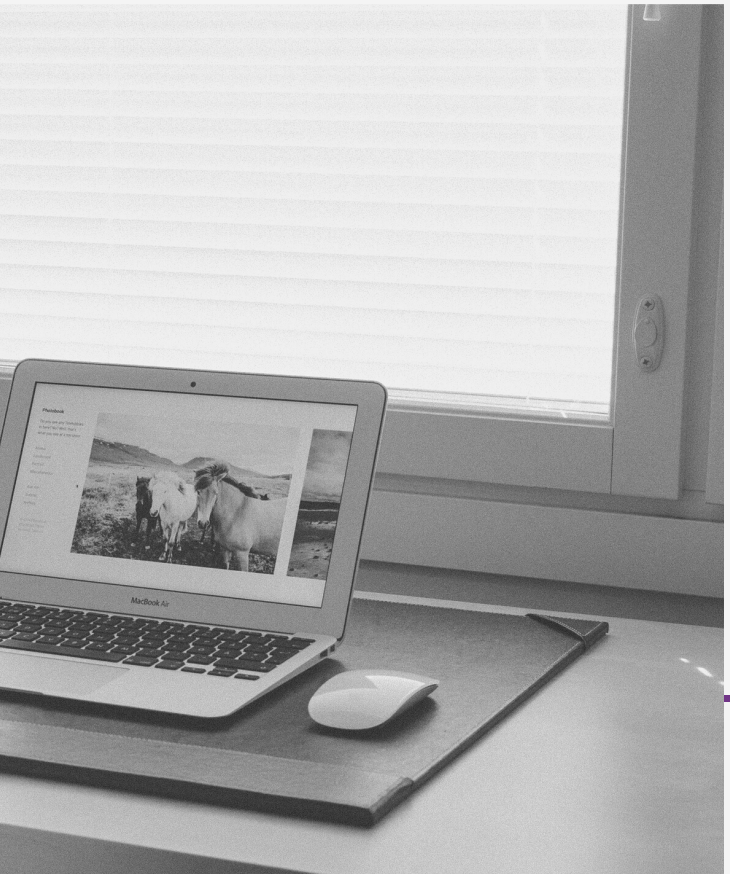
GDPR DATA PROTECTION

WHEN IT COMES TO A PERSONAL DATA BREACH, IT MEANS A BREACH OF SECURITY LEADING TO THE ACCIDENTAL OR UNLAWFUL DESTRUCTION, LOSS, ALTERATION, UNAUTHORISED DISCLOSURE OF, OR ACCESS TO, PERSONAL DATA.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. If you experience a personal data breach you need to consider whether this poses a risk to people.

You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report.

If not done properly, you can be fined 4% of your annual worldwide turnover or £18 million whichever is higher..



Therefore you need to be prepared for any potential data breach. The only way to do this is to have specific policies in place to cover all procedures which you carry out. These are designed to assist with the smooth running of your business, thus allowing co-operation and ease of trading. We will cover these policies later in the guide.

It is essential that you know exactly where the subject's data is being stored. This is needed should the data subject make a request to see this data and if you don't know where it is, you will be unable to comply.

In addition, you will need to have in place good backup and disaster recovery procedures and therefore the location of the data is required.

There are an increasing number of services offering ‘cloud storage’ where you can upload documents, photos, videos and other files to a website to share with others or to act as a backup copy. This means you need to check that the security and availability of the service is right for the types of files you want to upload.

Security of your clients data is at the heart of GDPR. If your clients data is not secured, there is more chance of a data breach. You should review (and improve, if necessary) your current security arrangements in your office or home working environment.

Your clients or staff have the right to be informed if their personal data is being used. In turn, you have the right to ask an organisation whether or not they are using or storing your personal information. You can also ask them for copies of your personal information, verbally or in writing.

This is called the right of access and is commonly known as making a subject access request or SAR. When an organisation responds to your request, they should normally tell you whether or not they process your personal information and, if they do, give you copies of it.

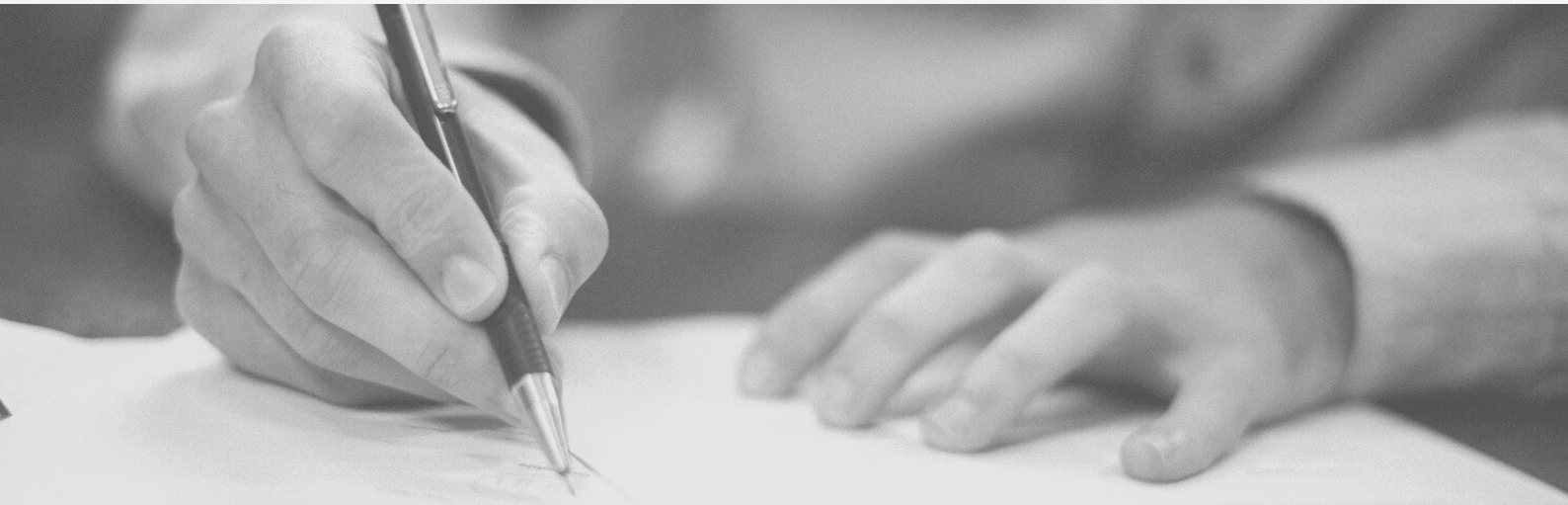
"YOU NEED TO BE ABLE TO EASILY IDENTIFY WHETHER YOU'RE RELYING ON CONSENT TO PROCESS PERSONAL DATA. THE CONSENT FOR PERSONAL DATA NEEDS TO BE CLEAR, SPECIFIC AND EXPLICIT."

When it comes to GDPR you simply need to know everything about your data. You need to demonstrate an understanding of the types of personal data (for example name, address, email, bank details, photos, IP addresses) and sensitive (or special category) data (for example health details or religious views) you hold, where they're coming from, where they're going and how you're using that data.

You need to make sure you have adequate security measures and policies. You need to update these to be GDPR-compliant, and if you don't currently have any, get them in place.

Broad use of encryption could be a good way to reduce the likelihood of a big penalty in the event of a breach. You should be able to provide what personal data you have on a person if they request access and this should be provided within a one-month timeframe. The people who you hold personal data on are allowed to access all of their personal data, rectify anything that's inaccurate and object to processing in certain circumstances, or completely erase all of their personal data that you may hold. Each request carries a timeframe and deadline of one month (which can only be extended in mitigating circumstances), from the original date of request.

You will need to train your employees, and report a serious breach within 72 hours. Ensure your employees understand what constitutes a personal data breach and build processes to pick up any red flags. It's also important that everybody involved in your business is aware of a need to report any mistakes to you as the owner of the company or to a Data Protection Officer or the person or team responsible for data protection compliance, as this is the most common cause of a data breach. This means you need to decide if you need to employ or make someone a Data Protection Officer (DPO). Most small businesses will be exempt.



HOWEVER, IF YOUR COMPANY'S CORE ACTIVITIES INVOLVE...

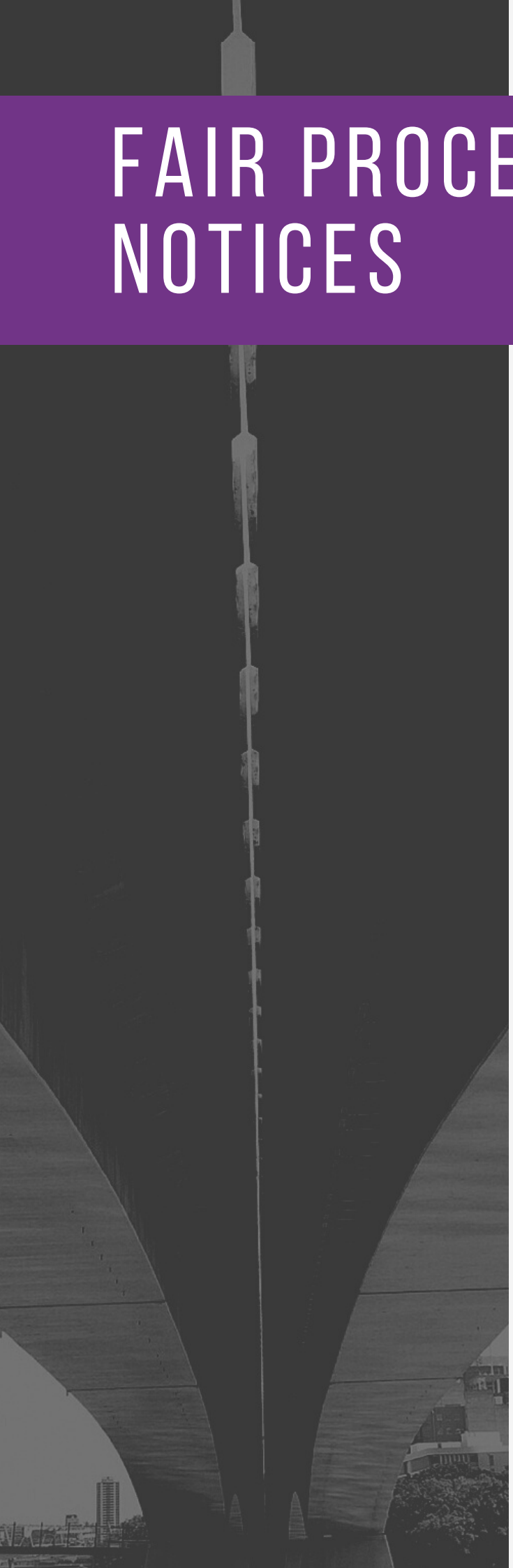
'regular or systematic' monitoring of data subjects on a large scale, or which involve processing large volumes of 'special category data' you must employ a Data Protection Officer (DPO).

Data controllers are obliged to keep written records of data processing activities.

These policies should cover all aspects of the business and should include the contact details of the data controller, data processing officer (DPO) or designated person within your business.

Conduct due-diligence on your supply chain.

You should ensure that all suppliers and contractors are GDPR-compliant to avoid being impacted by any breaches and consequent penalties. You also need to ensure you have the right contract terms in place with suppliers (which puts important obligations on them, such as the need to notify you promptly if they have a data breach).



FAIR PROCESSING NOTICES

You will need to create fair processing notices. Under GDPR, you're required to describe to individuals what you're doing with their personal data. It is a good idea to have a folder with all the policies in it, somewhere in the office that is easily accessible for reference. There are specific sets of policies depending on the type of business and the size e.g. sole trader, SME and corporate. It is all very well making up policies and procedures but it defeats the purpose of the whole exercise if they are not implemented. Users within the company must be made aware of these policies and that should form the basis of training. Once training is given, staff should sign off that they have understood the concepts of GDPR and are aware of procedures should anything happen that require action.

ONCE THE POLICIES HAVE BEEN IMPLEMENTED...

they should be revised periodically and updated where necessary.

In our data-driven world, it's more important than ever to know who is using your personal data, and why. It's your right to be informed about how organisations are using your data, even if it happens behind the scenes. This includes understanding how people use your data to target you with social media adverts.

Our aim at The Business Train is to deliver a consistent educational message that will help you understand the changing data protection environment in a practical and straightforward way.

Regardless of your industry or size, we can help complement your own customer and staff GDPR communications. We hope to ease the burden on you having to create your own materials while at the same time ensuring a coherent message is communicated.

When it comes to GDPR it is important to understand what a personal data breach means so that you can be prepared for it.

Which means you need to know how to recognise a personal data breach. A personal data breach isn't only about loss or theft of personal data.

It's about being prepared and having a response plan for addressing any personal data breaches that occur.

Either you or someone within your company needs to be allocated responsibility for managing any breaches. Your staff need to know who this person is so they know how to escalate a security incident so you can determine whether a breach has occurred.

In the event of a personal data breach you need a process to assess the likely risk to individuals as a result of the breach. You know who the relevant supervisory authority is for your processing activities. Then you need a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if you do not have all the details yet. You need to know what information you must give the ICO about a breach.

You need a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

You need to know how to inform affected individuals without undue delay. You need to know what information about a breach you must provide to individuals, and that you should provide advice to help them protect themselves from its effects.You must document all breaches, even if they don't all need to be reported. When reporting a breach, the GDPR says you must provide a description of 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, including, where appropriate, the measures taken to mitigate any possible adverse effects.

DEPENDING ON THE SIZE OF YOUR BUSINESS

AND HOW MUCH PERSONAL DATA RECORDS YOU STORE.

You may need to carry out a system audit or DPIA (data protection impact assessment). A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. Under GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher.



SOLE TRADERS

The first thing you need to do as a business owner is register your company with the ICO. From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader who processes personal information to pay a data protection fee to the ICO. This is a small fee and can be done online, it takes about 20 minutes and you will need some basic information about your business.

Although, if you are a sole trader, and you are not using CCTV or processing any personal data electronically, you are exempt. This means you do not have to pay a fee to the ICO.

GDPR BREACH CONSEQUENCES

SO WHEN IT COMES TO A DATA BREACH THERE ARE DIFFERENT TYPES. THE MOST COMMON IS A PERSONAL DATA BREACH THAT LEADS TO THE ACCIDENTAL OR UNLAWFUL DESTRUCTION, LOSS, ALTERATION, UNAUTHORISED DISCLOSURE OF, OR ACCESS TO, A CUSTOMER/ CLIENT OR STAFF MEMBERS PERSONAL DATA.

If you experience this type of personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report. You do not need to report every breach to the ICO.

But bare in mind, without the right legal documents or failing to report something that is a defined breach, you could face a criminal prosecution. Therefore if you employ staff, they must undergo some form of training. It is your responsibility to make sure your staff are trained as this is a typical area where you as a business owner get exposed. We suggest that you hold an initial training session for all staff to make sure they are aware of GDPR and how it may affect them in their day to day job. This needs to continue periodically, every 6-8 months but at least once a year. It is also vital to train new staff and to make sure they go through an induction, that includes GDPR. The GDPR requires you to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR provides more specifics about what you have to do about the security of your processing and how you should assess your information risk and put appropriate security measures in place. Whilst these are broadly equivalent to what was considered good and best practice under the 1998 Act, they are now a legal requirement.

A core weakness in a business are the computers and not just on-site machines. Using cloud storage services means that you and others can access and share files across a range of devices and locations. Files such as photos and videos can sometimes be difficult to email if they are too large or you have a lot of them. Uploading to a cloud storage provider means you can quickly circulate a URL and you can share your files with anyone you choose.

You might also use cloud storage services to keep copies of important files outside your home as part of a backup solution. This means that in the event of a disaster in your home (eg fire, flood or theft) you still have copies of your data.

Your IT Security needs to be reviewed, especially when it comes to storing personal data. The majority of business owners use simple virus software and think they are safe. It becomes a lot more complicated with firewalls and passwords, or when staff write a password on a notepad for example. This means other people can see it which may lead to a breach. In this day and age, where hacking and cyber crime are on the increase, more stringent measures of security must be put in place.

FILING CABINETS

"WE GET ASKED A LOT ABOUT FILING CABINETS. THERE IS A REQUIREMENT TO PROTECT DATA THAT IS NOT ELECTRONICALLY STORED I.E. HAVING PAPERS LYING ABOUT."

A clear desk policy should be adopted and each evening, all relevant paperwork should be locked in filing cabinets each evening.

A breach may not be your fault but can occur due to a 3rd party supplier not having the correct procedures in place. It is your duty to check if the supplier is GDPR compliant and it is always a good idea to put in place a 3rd party agreement. It is a good practice to carry out due diligence on any supplier with whom you engage.

NOW YOU CAN SEE WHY YOU MUST PROTECT YOURSELF...

by putting good practices in place and using the ICO guidelines to help you mitigate any problems. If you follow these guidelines and even though you have done everything properly, you may still suffer a breach, but it will go in your favour that you have done everything possible to comply. Because you can show you have tried your best, you may escape a fine, but only if you carry out these necessary steps.

Almost every transaction and interaction you have with most organisations involves you sharing personal data, such as your name, address and birth date.

You share data online too, every time you visit a website, search for or buy something, use social media or send an email.

Sharing data helps make life easier, more convenient and connected. But your data is your data. It belongs to you so it's important your data is used only in ways you would reasonably expect, and that it stays safe. Data protection law makes sure everyone’s data is used properly and legally.

You have the right to ask an organisation whether or not they are using or storing your personal information. You can also ask them for copies of your personal information, verbally or in writing.This is called the right of access and is commonly known as making a subject access request or SAR

Typically when you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing, this falls under legitimate interests. This is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.

Which is why we provide our documentation toolkits that make all of this easier to understand and allows you to have the correct documents and procedures in place for your individual company requirements. Once your registration with the ICO is complete, it's a good idea to contact us so that we can assess what policies you will require to be protected from any potential data breaches.

These policies could be a mix of the below:

- Data Protection Policy
- Privacy Notice
- Data Breach Incident Form
- Data Breach Policy
- Data Retention and Erasure Policy
- SAR Acknowledgement
- SAR Response S
- AR Partial Exemption
- SAR Denied S
- AR Delayed
- SAR Procedures
- Access Control and Password Policy
- BYOD and Remote Access Control
- Clear Desk Policy
- eMail Usage and Archive Policy
- Information Asset Register
- Asset Management Policy
- Information Security Policy
- Risk Management Policy and Procedures
- Risk Mitigating Action Plan
- Outsourcing and Supplier Policy
- Employee Training Record
- Training Development Log
- Training Development Policy
- Training Feedback Form
- Supplier and Due Diligence Questionnaire

You are able to fill in and update the above templates but we are more than happy to assist with them.

There may be others that you require depending on your circumstances.

We also provide personal services to assist in the personalisation of these policies.We can carry out an audit of all your systems and continue to support you in case of a breach or any updates required in the future.

We can also help with your staff training, as a big percentage of breaches come from employees in one form or another. We can provide the training required so that your staff are aware of their responsibilities in respect of GDPR.

GDPR POLICIES

TO BE FULLY GENERAL DATA PROTECTION REGULATION COMPLIANT YOU ARE REQUIRED TO HAVE SPECIFIC POLICIES IN PLACE. FOR EXAMPLE, OFTEN YOU SEE COMPANIES WHO THINK HAVING A PRIVACY POLICY AND A CONSENT FORM ON THEIR WEBSITE IS ENOUGH; HOWEVER, THIS IS ONLY A SMALL PART OF THE DOCUMENTS THAT ARE REQUIRED.

We have created a list of the top GDPR documentations that are required. Please note that the names of these documents are not prescribed by the GDPR, so you may use some other titles; you also have a possibility to merge some of these documents.

Here are the documents that you must have if you want to be fully GDPR compliant:

1. TERMS AND CONDITIONS OF WEBSITE USE POLICY

Make sure your websites terms of use are up to date and easily accessible on your website. They should contain provisions dealing with access to, and use of, the website including information about the website owner, rights to modify or withdraw the website, disclaimers for material published on it or linked to from it and rules about how such materials may be used.

2. PRIVACY NOTICE TO STAFF POLICY

This privacy notice is for use by employers to advise employees, workers, contractors and other individuals who are employed or engaged by the business about the collection, storage and use of personal data by the employer. A privacy notice should be given to everyone whose data is collected and processed, including job applicants.

3. EMPLOYEE PRIVACY NOTICE POLICY

This explains how your company is going to process personal data of your employees (which could include health records, criminal records, etc.).

4. DATA RETENTION POLICY

A data retention policy establishes and describes how a company expects its employees to manage personal data. GDPR states that personal data shall be 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. This policy will help businesses identify and establish its own rules for how long data should be retained for.

5. PRIVACY POLICY AND COOKIE POLICY

This privacy policy is for use by a business in relation to the collection, storage and use of non-sensitive personal data, for use on a website which collects such data for the purpose of supplying goods or services to users of the site, or for contacting users with direct marketing information. This privacy policy also incorporates a cookie policy which provides internet users with the necessary information about an online provider's use of cookies as required by the Privacy and Electronic Communications.

6. DATA PROCESSING AGREEMENT POLICY

You should also have a GDPR compliant data processing agreement. It covers the obligations that parties need to comply with when using third parties to process personal data.

7. DATA PROCESSING CLAUSES POLICY

This document contains clauses to be inserted into a third party supply agreement where the third party is processing personal data. The clauses contain the relevant obligations to comply with GDPR.

8. DATA RETENTION POLICY

This describes the process of deciding how long a particular type of personal data will be kept, and how it will be securely destroyed.

9. DATA RETENTION SCHEDULE POLICY

This lists all of your personal data and describes how long each type of data will be kept.

10. DATA SUBJECT CONSENT FORM

GDPR contains rules on how a business should obtain consent. This document contains a range of consents and guidance notes on how to use each consent form. This is the most common way to obtain consent from a data subject to process his/her personal data.

11. DATA PROTECTION POLICY

This is a standard policy for use by a business setting out the principles and legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data used in the course of the operation and administration of the business, including customer, supplier and employee data.

12. IT SECURITY POLICY

This is a standard policy for use by a business setting out the IT and data security principles that a business must comply with under GDPR. Businesses are required to put in place appropriate technical and organisational measures in place to prevent personal data being damaged, lost or stolen.

13. DPIA REGISTER

This is where you'll record all the results from your Data Protection Impact Assessment.

14. SUPPLIER DATA PROCESSING AGREEMENT

This is where you need to regulate data protection with a processor or any other supplier.

15. DATA BREACH RESPONSE AND NOTIFICATION PROCEDURE POLICY

This describes what to do before, during, and after a data breach.

16. DATA BREACH REGISTER

This is where you'll record all of your data breaches. (Hopefully, it will be very short.)

17: DATA BREACH NOTIFICATION FORM TO THE SUPERVISORY AUTHORITY

In case you do have a data breach, you'll need to notify the Supervisory Authority in a formal way.

18: DATA BREACH NOTIFICATION FORM TO DATA SUBJECTS

Again, in case of a data breach, you'll have the unpleasant duty to notify data subjects in a formal way.

19. CLAUSES FOR STAFF AGREEMENTS

These clauses for staff agreements have been updated to reflect GDPR, given the new rules on consent in an employment relationship. If you are issuing agreements to new members of staff or amending contracts for some other reason from 25th May 2018, these clauses can be used.

20. EMPLOYEE CONSENT FORM

GDPR rules on consent in an employment relationship mean that it would not normally be appropriate to request that an employee give their consent to their employer for their data to be processed. However, there may be limited and specific circumstances when this is required.

21. MEMORANDUM TO BOARD OF DIRECTORS

The board of directors of a company needs to understand GDPR and have overall responsibility for a company's compliance with GDPR. This memorandum highlights the key areas that the company needs to understand with regard to GDPR so that the board understands the implications of failing to comply with GDPR.

Even though it might seem overwhelming

with all of these policies, you really can implement GDPR by yourself.

All you need is 1 of our documentation toolkits, along with our included guidance and support. Our toolkits and other resources were developed for ease of use and to be understandable, with no expert knowledge required.

What's more, here at the The Business Train, we eliminate the stress and headaches that can come with doing it yourself, and you'll eliminate the huge price tag that comes with a consultant.

We've calculated your savings, and we estimate that you will save over 90% compared to the cost of a lawyer or consultant. In other words, you'll save thousands of pounds – with no drop in quality!

The policy documents we supply you with are organised to guide you on your implementation path. They're structured in clearly numbered folders, so that you know where to start, and – after each document is completed – where to go next.
We've done 80% of the work a consultant would charge you for. Anything that can be prefilled in the documents is already done, and the remaining adaptation you need to do is clearly marked with comments and instructions.
EU GDPR compliance is much more than just documentation. The implementation of this regulation needs to be appropriate to your company, and you need to deal with your employees, your management, and your existing processes in an appropriate way.
This is why our we are on hand with support to answer any difficult questions – we can set up a call via Skype, Zoom, over the telephone, or through any other method convenient for you; or, we can answer your questions via email – whatever suits you best.

As part of your DPIAs, you should be asking ‘what am I going to check to make sure that everything is as it should be.’ You should be sure that where the logs retain personal data that you know for how long you are retaining them. It may be that the logs themselves are the core part of processing personal data.

If you are responding to incidents relating to security or breaches The Business Train has a range of advice. Once you have a logging strategy in place, you will be better prepared for the most pressing questions put to you by incident investigators should you suffer a cyber-attack. This will give you the best chance of recovering swiftly, and to defend your systems better against future incursions.

You should know what is recorded, why and make sure it is only kept for the period you need it for. If you are completing DPIAs, then this will help gather that information.

CORPORATE

If you are a corporate business, you would need to carry out an audit lasting between 1 to 3 days. It may be that you need a DPIA, which is a tool to help you identify and minimise the data protection risks of new projects.

They are part of your accountability obligations under the GDPR, and an integral part of the ‘data protection by default and by design’ approach.

We are able to assist in the personalisation of your policies, once we carry out an audit of all systems. After that is complete, we will continue to support you in case of a breach or any updates required to the policies.

It is imperative that your staff are trained, as a big percentage of breaches come from employees in one form or another. We can provide the training required so that staff are aware of their responsibilities in respect of GDPR.

STEP 2

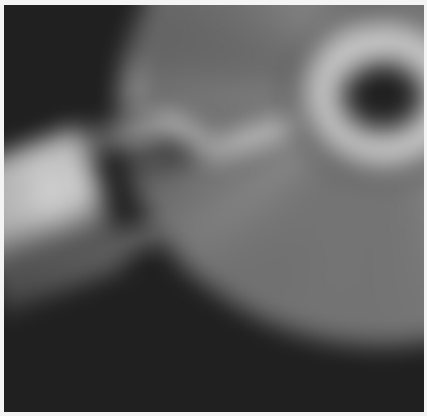
GDPR OVERVIEW

"KNOW WHAT YOU ARE DOING"

GENERAL DATA PROTECTION REGULATION

When it comes to General Data Protection Regulation and making sure your business is compliant you will need to be aware of the many different policies and procedures. You can start with the data you are holding, where it is stored and how it is protected and what kind of software or technology is in place to protect it.
You will need to review your current data-related policies, including encryption, remote access, mobile devices, sensitive information, HR exit procedures, third parties and data breach notifications.
You might need a third-party data security company to carry out an objective assessment.
You will need to identify if you have any risks of a data breach.

You will need to think about your customers individuals' rights and be prepared for transferring personal data to other companies and to delete personal data if requested. Are requests for permission to use customers' personal data clear on the purpose and period of time?We at the Business Train can help you find solutions for any identified risks or gaps.Solutions that can be implemented as soon as possible. You may need to designate a Data Protection Officer or lead contact. A DPO can be appointed if mandatory for the business, or an internal lead contact person can be appointed for data protection initiatives and to communicate with the Data Protection Authority if required.



DATA PROTECTION OFFICER

You may need to designate a Data Protection Officer or lead contact. A DPO can be appointed if mandatory for your business, or an internal lead contact person can be appointed for data protection initiatives and to communicate with the Data Protection Authority if required.The DPO or lead contact should communicate with senior management to discuss data protection strategies and you will need to make sure you have provided staff training and awareness. It is important that your staff are aware of the importance of data protection and any new/amended processes to comply with the GDPR.

You will need to make sure any internal teams are communicating with each other so you can maintain your data protection, such as IT, Security, Legal and Compliance teams.Even though this might seem overwhelming at first, GDPR compliance can easily be achieved by having the right policies and procedures in place. We make this very easy for you by offering a specific GDPR policy bundle. These policies can simply be filled in with your details and you will be fully compliant and ready for any unexpected data breaches.

GDPR AND YOUR BUSINESS

THE FIRST THING THAT YOU SHOULD DO AS A BUSINESS OWNER IS WORK OUT WHAT NEEDS TO BE DONE TO COMPLY WITH GDPR. IT IS POSSIBLE THAT YOU MAY ALREADY COMPLY WITH SOME OF THE REQUIREMENTS, EVEN THOUGH YOU WERE NOT AWARE OF WHAT NEEDED TO BE DONE.

For example, your IT department may already have good structures in place with regards to such things as password control, anti-virus and anti-malware software and cyber security as a whole.The best way of determining all these things, is to carry out a system audit or DPIA (data protection impact assessment).

DATA PROTECTION IMPACT ASSESSMENT

"YOU MAY BE DAUNTED BY THIS AS IT IS SUCH AN EXTENSIVE EXERCISE BUT IT IS REALLY THE BEST WAY TO PROCEED. IF THAT IS THE CASE, YOU MAY WISH TO CONSIDER BRINGING IN SOMEONE TO CARRY THIS OUT ON YOUR BEHALF."

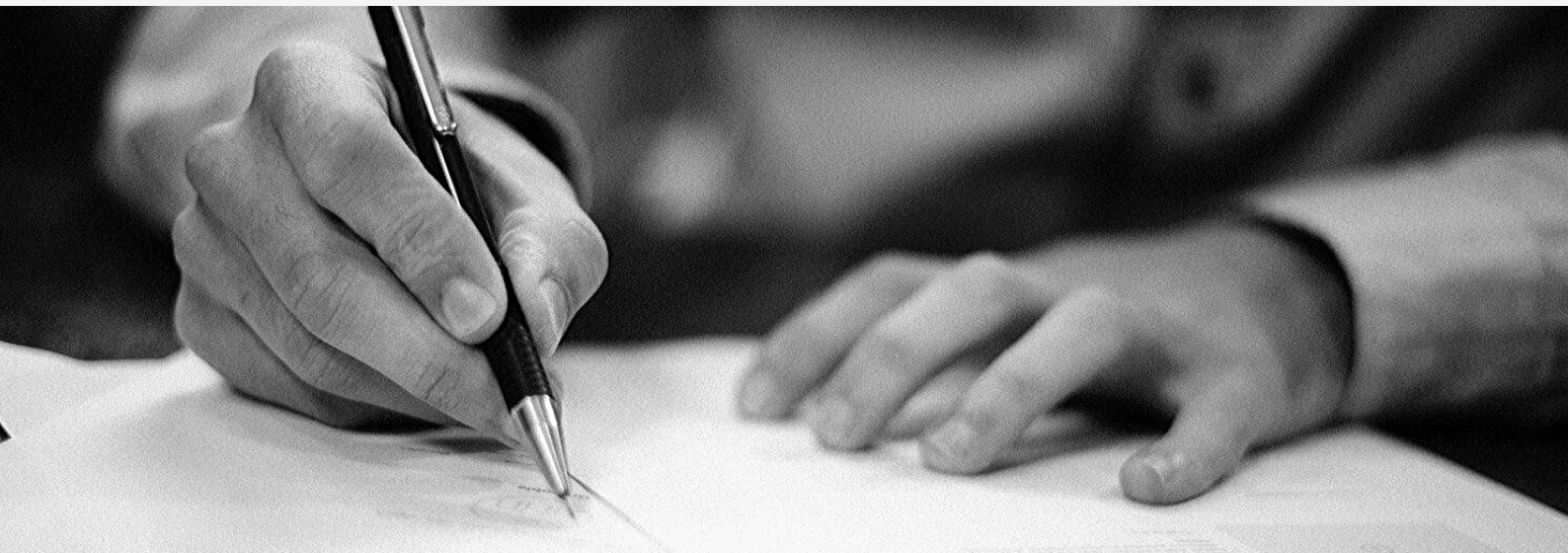
A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

DPIA's are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

There is no definitive DPIA template that you must follow. You can use our suggested template if you wish, or you may want to develop your own template and process to suit your particular needs, using our guidance as a starting point.
DPIA's are an essential part of your accountability obligations.

Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher. Resources therefore must be allocated so as to implement GDPR effectively. Roles and responsibilities within the company must be clearly defined, and you should ascertain whether or not you need to appoint a DPO.



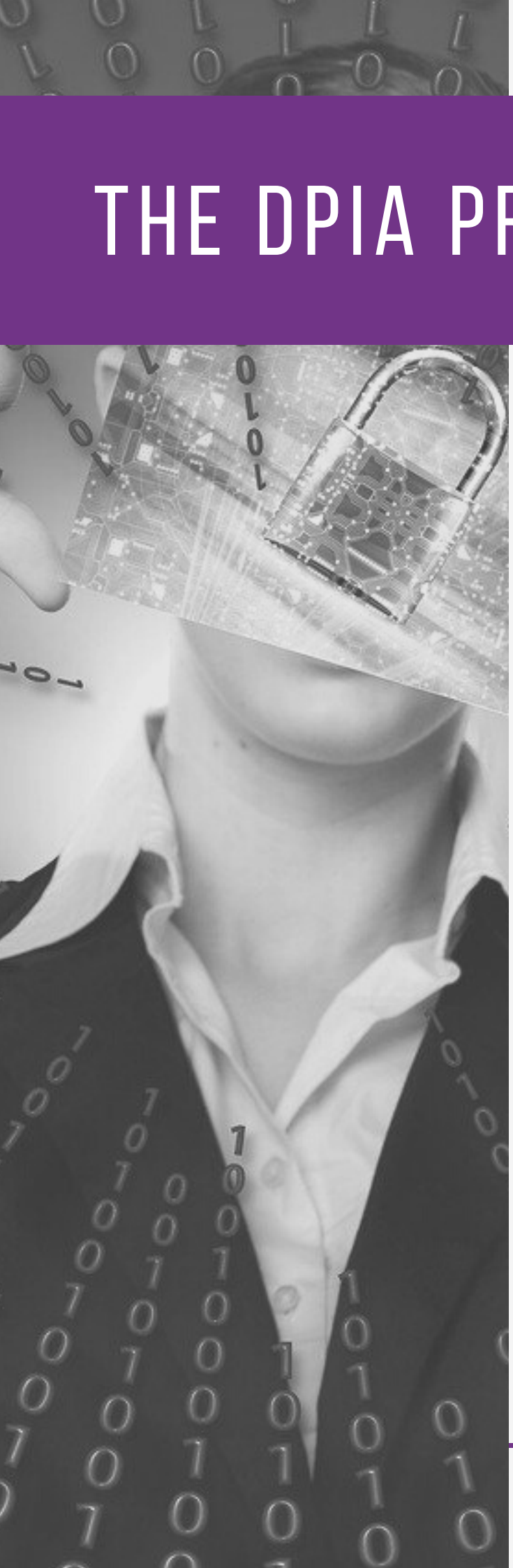
A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process.

If not, it is still a good idea to put in place a designated person.
The audit should also find out the extent to which each of the GDPR's processing principles are accounted for in each process that involve personal data, and which lawful basis for that processing is identified. It should also identify the processes your organisation has implemented to facilitate and respond to data subjects exercising their rights under the GDPR.

A DPIA should include these steps:

Step 1: identify the need for a DPIA
Step 2: describe the processing
Step 3: consider consultation
Step 4: assess necessity and proportionality
Step 5: identify and assess risks
Step 6: identify measures to mitigate the risks
Step 7: sign off and record outcomes

THE DPIA PROCESS



After sign-off you should integrate the outcomes from your DPIA back into your project plan, and keep your DPIA under review. Throughout this process, you should consult individuals and other stakeholders as needed.

The DPIA process is designed to be flexible and scalable. You can design a process that fits with your existing approach to managing risks and projects, as long as it contains these key elements.

You can also scale the time and resources needed for a DPIA to fit the nature of the project. It does not need to be a time-consuming process in every case.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.
If the ICO accept your DPIA, they don't just look at the risks you documented. They consider all of your submission – your DPIA documentation and any further information you provided – along with any prior contact you may have had with their office.

The ICO seek to understand in detail the context and nature of the processing you are proposing, including any controller-processor relationships. They will also assess the extent to which you have evidenced compliance with the Data Protection Principles.

Unlike large businesses, sole traders don't need to appoint a Data Protection Officer. However, you could be fined up to 4% of your annual turnover for failing to get sufficient consent to collect or keep data. In fact, even failure to keep accurate data records could result in a fine of up to 2% of annual turnover.

It's fair to say that this subject can seem very complex, however it relies on being clear with people about the data you collect and keep.

You need to be specific about the information you are taking, what you will do with it and who else might see it. Importantly, people need to be given the chance to positively ‘opt-in’, having made a clear choice that they agree to their details being taken. That means that they shouldn’t be presented with pre-ticked boxes or default options on forms they fill in, for instance.Records of data consent need to be kept and it should be easy for individuals to withdraw their consent whenever they wish. People have the ‘right to be forgotten’ if they no longer want their data to be held.

GDPR REQUIREMENTS

SO LET'S GET A BETTER UNDERSTANDING ABOUT YOUR GDPR REQUIREMENTS AND SOME OF THE CORE PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA THAT YOU NEED TO BE AWARE OF.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(A) CONSENT:

The individual has given clear consent for you to process their personal data for a specific purpose. The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes.

It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. You must keep clear records to demonstrate consent. The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement.

But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair. Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told. Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

(B) CONTRACT:

The lawful basis for contracts to apply is when you are processing a data subject that is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract. You can rely on this lawful basis if you need to process someone's personal data to deliver a contractual service to them; or because they have asked you to do something before entering into a contract (eg provide a quote). The processing must be necessary. If you could reasonably do what they want by processing less data, or using their data in a less intrusive way, this basis will not apply.You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

(C) LEGAL OBLIGATION:

The processing is necessary for you to comply with the law (not including contractual obligations).

You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation. This does not apply to contractual obligations. The processing must be necessary.

If you can reasonably comply without processing the personal data, this basis does not apply.You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning. You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

(D) VITAL INTERESTS:

You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.

You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
You should consider whether you are likely to rely on this basis, and if so, document the circumstances where it will be relevant and ensure you can justify your reasoning.

(E) PUBLIC TASK:

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

You can rely on this lawful basis if you need to process personal data:'in the exercise of official authority'. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law. It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law. The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.

Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

(F) LEGITIMATE INTERESTS:

This is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to identify a legitimate interest; show that the processing is necessary to achieve it; and balance it against the individual's interests, rights and freedoms. The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required. You must include details of your legitimate interests in your privacy information.

You must tell people in your privacy information

that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.
If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects.

For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights.

When it comes to your GDPR requirements, there are some core principles for the processing of personal data to be aware of.

Whenever you process personal data, you need to make sure that an individual has given you clear consent for you to process their personal data for a specific purpose.

The lawful basis for contracts will apply if you need to process someone's personal data to deliver a contractual service to them; or because they have asked you to do something before entering into a contract (eg provide a quote).

PEOPLES DATA...

Typically when you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing, this falls under legitimate interests. This is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.

This is why we provide our documentation toolkits to make all of this easier to understand and allows you to have the correct procedures in place for your individual company requirements.

As an SME business owner, see if you have already done the following 10 steps:

- Made sure all your key decision makers in your business are aware of GDPR.
- Documented all the data you hold, where you got it from and who has access to it.
- Reviewed your privacy notices you issued when collecting data
- Checked to ensure you cover all eight rights for individuals covered by the rules.
- Developed a plan for dealing with data requests
- Written up a document showing how you'll lawfully use data
- Reviewed how you seek, record and manage consent to take data
- Have an action plan to react to a data breach (including details of your cyber insurance)
- Read up on the ICO's 'Privacy Impact Assessments'
- Appointed a data protection officer (if you're a big business or involved in the large scale processing of data)

GDPR ACCOUNTABILITY

ACCOUNTABILITY IS ONE OF THE DATA PROTECTION PRINCIPLES, WHICH MEANS YOU ARE RESPONSIBLE FOR COMPLYING WITH GDPR AND MUST BE ABLE TO DEMONSTRATE YOUR COMPLIANCE.

You need to put in place appropriate technical and organisational measures to meet the requirements of accountability. There are a number of measures that you can, and in some cases must take including adopting and implementing your data protection policies.

YOU MUST PUT WRITTEN CONTRACTS IN PLACE...

With organisations that process personal data on your behalf. You need to maintain documentation of your processing activities and implement appropriate security measures. You will be required to record and, where necessary, report personal data breaches to the ICO. You will need to have proof that you have carried out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests. Depending on the size of your company, you will need to appoint a data protection officer who adhere to relevant codes of conduct and signs up to the correct certification schemes.

GDPR ACCOUNTABILITY OBLIGATIONS

These GDPR accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place. If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.

Being accountable can help you to build trust with individuals and may help you mitigate and future enforcement action. Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

You must report certain types of personal data breach to the relevant supervisory authority such as the ICO, and in some circumstances, to the affected individuals as well.

ADDITIONALLY, THE GDPR SAYS THAT YOU MUST KEEP A RECORD OF ANY PERSONAL DATA BREACHES, REGARDLESS OF WHETHER YOU NEED TO REPORT THEM OR NOT.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this. The GDPR contains explicit provisions about documenting your processing activities. You must maintain records on several things such as processing purposes, data sharing and retention.

You may be required to make the records available to the ICO on request.

Documentation can help you comply with other aspects of the GDPR and improve your data governance. Controllers and processors both have documentation obligations. For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.

Documentation can help you comply...

With other aspects of the GDPR and improve your data governance. Controllers and processors both have documentation obligations. For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities. Information audits or data-mapping exercises can feed into the documentation of your processing activities. Records must be kept in writing. Most organisations will benefit from maintaining their records electronically.

Records must be kept up to date and reflect your current processing activities. We have produced some basic templates to help you document your processing activities.

The principle of accountability aims to guarantee compliance with the Data Protection Principles. It implies a cultural change which endorses transparent data protection, privacy policies & user control, internal clarity and procedures for operationalising privacy and high level demonstrable responsibility to external stakeholders & Data Protection Authorities.

The GDPR requires that the controller is responsible for making sure all privacy principles are adhered to. Moreover, the GDPR requires that your business can demonstrate compliance with all the principles. So, what steps should your business take to build such a culture and to be able to demonstrate accountability?

THERE ARE SIX PRINCIPLES

There are six principles set out in the GDPR. These are the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. One of the best ways to make sure these principles are adhered to is to make sure your internal privacy governance structure is set up correctly and comprehensively.

The ways to incorporate these principles are woven in throughout the GDPR.

"For instance, the GDPR states your business is required to deploy appropriate technical and organisational measures as laid out in the GDPR."

Such as documented processes/policies, data protection impact assessments (DPIA), suggested data security methods, data protection by design and by default, a mandatory data protection officer (DPO) for large scale personal data processing, and keeping records of your processing activities.

Special attention is given to (industry) code of conducts and self-certification, data breach notification and transparency requirements.

Your data is central to the success of your business and if you hold important data on your staff and clients then you need to abide to the tough data protection laws that the General Data Protection Regulation (GDPR) have put in place. That way if there is ever a data breach or incident you can avoid any significant fines and huge reputational damage.

We will help you make sure your use of data is legally sound, advising on all facets of data protection – including GDPR, compliance, drafting policies, assisting with Privacy Impact Assessments and handling that 'worst case scenario'

We will help you take a proactive approach, ensuring your affairs are in order, your staff are trained and you are aware of all your risks and responsibilities.

You need to be confident you are meeting your obligations under the General Data Protection Regulation (GDPR) in respect of client, customer and employee personal information and have appropriate policies, procedures and cyber-security measures in place.

STEP 3

GDPR COMPLIANCE

"KNOW WHAT YOU ARE DOING"

REGISTER YOUR COMPANY WITH THE ICO

The first thing to do is register your company with the ICO. From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation who processes personal information to pay a data protection fee to the ICO, unless they are exempt. Some of the information you provide on the register of controllers is published for all to see. If you use a domestic address in the course of your business and do not wish for this to be included on the public register which is available and downloadable from our website, you should provide a PO Box or alternative address instead.

When it comes to owning an SME business the ICO categorize you into three different tiers.

Tier 1 is called a micro organisation, this is where you have a maximum turnover of £632,000 for your financial year or no more than 10 members of staff. If your business falls into this tier you only need to pay £40 a year.If your business has a maximum turnover of £36 million for your financial year or no more than 250 members of staff, you fall into Tier 2 and would need to pay £60 a year. If you do not meet tier 1 or tier 2, you will need to pay the tier 3 fee of £2,900 a year.

Your fee covers a 12 month period

It’s important to know that you are breaking the law if, as a controller, you process personal data, or are responsible for the processing of personal data, for any of the non-exempt purposes and you have either:
not paid a fee, ornot paid the correct fee.

The maximum penalty is a £4,350 fine (150% of the top tier fee.)

Your fee covers a 12 month period from the renewal date.

As a corporate business owner you will need to fill out more templated legal policies which means it's important to become familiar with the legal terms.

USEFUL TERMS TO LEARN...

The following terms are mentioned a lot within the policies:

Controller: This is the person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.

Processor: This is the person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Subject: This is the identified or identifiable living individual to whom personal data relates.

Personal Data: This is any information relating to a person (a ' data subject ') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Processing: In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

Over 80% of breaches come from staff errors

If you have staff, you will need all the policies to cover them and then make sure they all get the necessary training. You will need to make sure your Data Protection Officer (DPO) this training or an outside agency can be brought in for this purpose.

As part of any staff induction, you or your DPO will need to make sure they are included in any documentation and then given the necessary training.

It is also important to have a staff handbook that can be updated on a regular basis so they have documentation to which they can refer.

In addition, if you outsource your IT support to an external person or company and they have access to your computers and therefore the data, they need to be GDPR compliant and it is up to you to establish this fact.

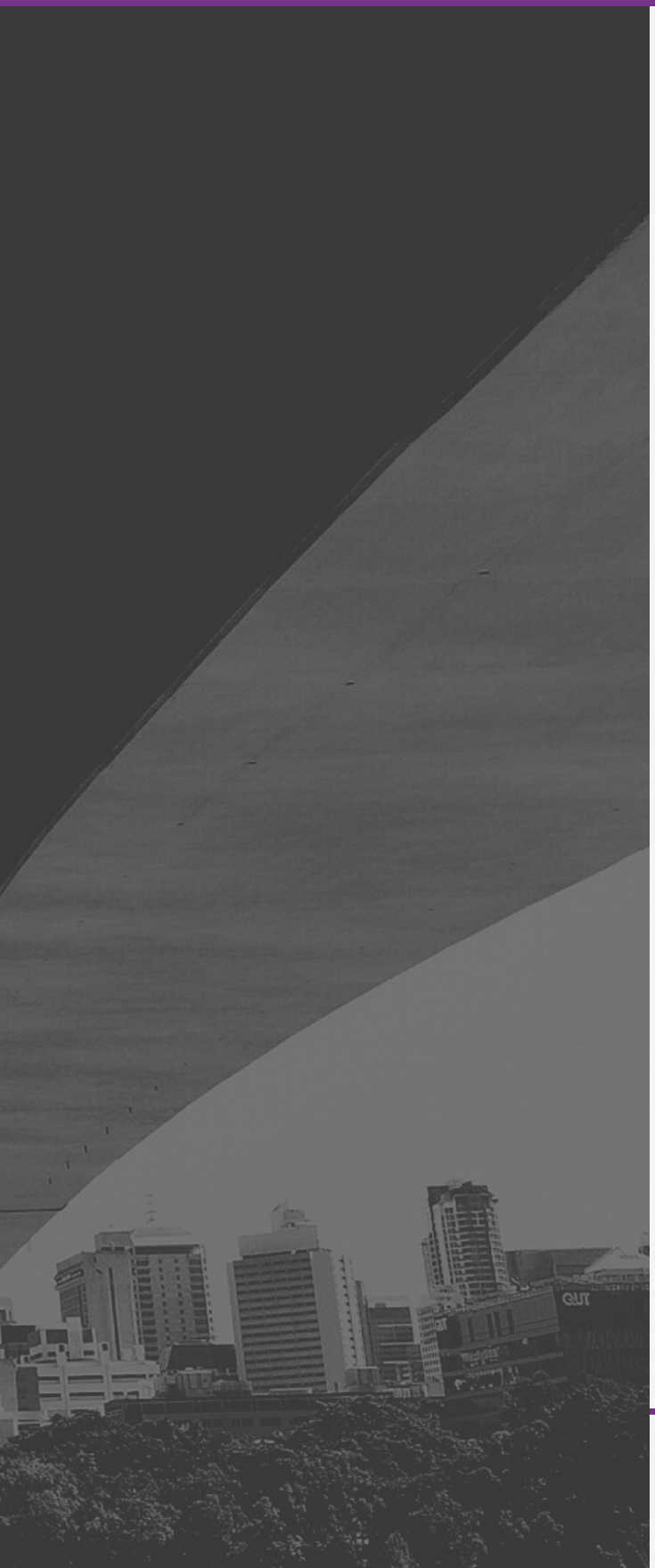
If your support is internal, you must be aware of what is required of the system so that they are GDPR compliant.

The easiest and fastest way to make sure everything is done correctly is to have an audit, or an DPIA.

The audit/ DPIA will ascertain the policies that are required and it is possible that they could be in excess of 30 to 40. Once your company has gone through an audit process, it is a good idea to book in GDPR review meetings once every 6-8 months.

To help start this whole process off we have created documentation toolkits that are designed to make the whole process much easier and a lot less overwhelming.

REGISTRATION SELF-ASSESSMENT:



Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioners Office (ICO), unless they are exempt.

By going through the questions you will be able to decide if you as an individual or on behalf of your business or organisation need to pay a fee to the ICO.

From 25 May 2018, people who use CCTV for domestic purposes, ie to monitor their property, even if it films beyond the boundaries of their property will be exempt from paying a fee under data protection law.

ON 1 APRIL 2019

THE RULES AROUND PAYING THE DATA PROTECTION FEE CHANGED.

Members of the House of Lords, elected representatives and prospective representatives (including police and crime commissioners) are exempt from paying a fee, unless they process personal data for purposes other than the exercise of their functions as a Member of the House of Lords, an elected representative or as a prospective representative.

Try the self assessment test yourself:

Click Here

If you are using CCTV or processing personal data electronically you will need to pay a fee to the ICO.

The ICO uses a form for organisations that need to pay a fee under the data protection legislation. It should take about 15 minutes to complete.

You will need to fill in this form in one session, so we suggest you get everything you will need to complete it before you start.

You will need:

- your credit/debit card or other payment details;
- details about the organisation(s) you are registering, eg Companies House number (if applicable), name, address;
- details about the number of staff you have and your turnover.

The ICO will use the information you provide to process your payment and maintain the public register. They will publish all the information you provide, except where we say otherwise.

Register here:

Click Here

POLICY TOOKIT 1 FOR SOLE TRADER:

IF YOU ARE A SOLE TRADER, AND YOU ARE NOT USING CCTV OR PROCESSING ANY PERSONAL DATA ELECTRONICALLY, THEN YOU ARE EXEMPT.

YOU THEREFORE DO NOT HAVE TO PAY A FEE TO THE ICO.

However, it is important that your organisation adheres to the principles of the General Data Protection Regulations and understands best practice for managing information. To help ensure you are complying with the GDPR, we have produced a range of training materials including practical toolkits, training videos and more. Even if you are exempt, you may still wish to pay a data protection fee.

Once your registration is complete, it is a good idea to contact us and explain your situation. This will help us to assess what policies you will require to be protected of any potential data breaches.

These policy templates are included in your toolkit 1:

- Data Protection Policy
- Privacy Notice Data Breach Incident Form
- Data Breach Policy
- Data Retention and Erasure Policy
- SAR Acknowledgement
- SAR Response
- SAR Partial Exemption
- SAR Denied
- SAR Delayed
- SAR Procedures

These policies can simply be updated with your company information and then held in folders within a secure location.

the business train
your journey starts here

CONTACT US TODAY

Even though it might seem overwhelming with all of these policies, you really can implement GDPR by yourself.

All you need is to purchase one of our documentation toolkits. Our toolkits and other resources were developed for ease of use and to be understandable, with no expert knowledge required.

alan@thebusinesstrain.co.uk

Direct mobile 07764 291731
Switchboard 0203 633 1967

POLICY TOOKIT 2 FOR SME BUSINESS:

IF YOU ARE A SME BUSINESS, AND YOU ARE USING CCTV OR PROCESSING ANY PERSONAL DATA ELECTRONICALLY, THEN YOU ARE NOT EXEMPT.

YOU THEREFORE HAVE TO PAY A FEE TO THE ICO.

However, it is important that your organisation adheres to the principles of the General Data Protection Regulations and understands best practice for managing information. To help ensure you are complying with the GDPR, we have produced a range of training materials including practical toolkits, training videos and more.

ARE YOU A SME BUSINESS?

If you are an SME Business, using CCTV or/and processing personal data electronically, you will need to pay a fee to the ICO.

You will need to fill in this form in one session, so we suggest you get everything you will need to complete it before you start.

Once your registration is complete or if you are already registered, it is a good idea to contact us so that we can assess what policies you will require to be protected from any potential data breaches.

You are able to fill in and update the templates but we are more than happy to assist with them. There may be others that you require depending on your circumstances.

These policy templates are included in your toolkit 2:

- Data Protection Policy
- Privacy Notice Data Breach Incident Form
- Data Breach Policy
- Data Retention and Erasure Policy
- SAR Acknowledgement
- SAR Response
- SAR Partial Exemption
- SAR Denied
- SAR Delayed
- SAR Procedures
- Access Control and Password
- Policy BYOD and Remote Access Control
- Clear Desk Policy
- eMail Usage and Archive Policy
- Information Asset Register
- Asset Management Policy
- Information Security Policy
- Risk Management Policy and Procedures
- Risk Mitigating Action Plan
- Outsourcing and Supplier Policy
- Employee Training Record
- Training Development Log
- Training Development Policy
- Training Feedback Form
- Supplier and Due Diligence Questionnaire

ADDITIONAL SERVICES:

We provide personal services to assist in the personalisation of the policies, once we carry out an audit of all systems. After that is complete, we will continue to support you in case of a breach or any updates required to the policies.of GDPR.

Training + HR:
It is imperative that your staff are trained, as a big percentage of breaches come from employees in one form or another. We can provide the training required so that staff are aware of their responsibilities in respect

Even though it might seem overwhelming with all of these policies, here at the The Business Train, we eliminate the stress and headaches that can come with doing it yourself, and you'll eliminate the huge price tag that comes with a consultant.

We've calculated your savings, and we estimate that you will save over 90% compared to the cost of a lawyer or consultant. In other words, you'll save thousands of pounds – with no drop in quality!

FREE ONE ON ONE CONSULTATION WITH A GDPR EXPERT

IS GDPR CREATING MORE QUESTIONS THAN ANSWERS?

The Business Train are offering a limited number of free consultations with a GDPR consultant to provide you with the clarification you need to make sure that your business is compliant with the new regulations.

If your journey has created more questions than answers or if you'd like to make sure your changes are adequate, we can help.

The Business Train has already worked with over 50 companies to get them moving towards full compliance, from a sole trader to a large corporate. This is an invaluable investment of time for any company, large or small, affected by the GDPR.

This offer is extremely limited and we recommend early application to avoid disappointment. Now that the GDPR requirements can be enforced, can you afford not to act?

the business train
your journey starts here

CONTACT US TODAY

Even though it might seem overwhelming with all of these policies, you really can implement GDPR by yourself.

All you need is to purchase one of our documentation toolkits. Our toolkits and other resources were developed for ease of use and to be understandable, with no expert knowledge required.

alan@thebusinesstrain.co.uk

Direct mobile 07764 291731
Switchboard 0203 633 1967

POLICY TOOKIT 3 FOR CORPORATE BUSINESS:

IF YOU ARE A CORPORATE BUSINESS, AND YOU ARE USING CCTV OR PROCESSING ANY PERSONAL DATA ELECTRONICALLY, THEN YOU ARE NOT EXEMPT.

YOU THEREFORE HAVE TO PAY A FEE TO THE ICO.

However, it is important that your organisation adheres to the principles of the General Data Protection Regulations and understands best practice for managing information. To help ensure you are complying with the GDPR, we have produced a range of training materials including practical toolkits, training videos and more.

ARE YOU A CORPORATE BUSINESS?

If you are a Corporate, using CCTV or/and processing personal data electronically, you will need to pay a fee to the ICO.

You will need to fill in this form in one session, so we suggest you get everything you will need to complete it before you start.

Once your registration is complete or if you are already registered, it is a good idea to contact us so that we can assess what policies you will require to be protected from any potential data breaches.

You are able to fill in and update the above templates but we are more than happy to assist with them. There may be others that you require depending on your circumstances.

These policy templates are included in your toolkit 3:

- Data Protection Policy
- Privacy Notice Data Breach Incident Form
- Data Breach Policy
- Data Retention and Erasure Policy
- SAR Acknowledgement
- SAR Response
- SAR Partial Exemption
- SAR Denied
- SAR Delayed
- SAR Procedures
- Access Control and Password
- Policy BYOD and Remote Access Control
- Clear Desk Policy
- eMail Usage and Archive Policy
- Information Asset Register
- Asset Management Policy
- Information Security Policy
- Risk Management Policy and Procedures
- Risk Mitigating Action Plan
- Outsourcing and Supplier Policy
- Employee Training Record
- Training Development Log
- Training Development Policy
- Training Feedback Form
- Supplier and Due Diligence Questionnaire

ADDITIONAL SERVICES:

If you are a corporate client, you would need to at least carry out an audit lasting between 1 to 3 days. It may be that you need a DPIA, which is a tool to help you identify and minimise the data protection risks of new projects. They are part of your accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach.

Support:
We are able to assist in the personalisation of the policies, once we carry out an audit of all systems. After that is complete, we will continue to support you in case of a breach or any updates required to the policies.

Training + HR:
It is imperative that your staff are trained, as a big percentage of breaches come from employees in one form or another. We can provide the training required so that staff are aware of their responsibilities in respect of GDPR.

Even though it might seem overwhelming with all of these policies, here at the The Business Train, we eliminate the stress and headaches that can come with doing it yourself, and you'll eliminate the huge price tag that comes with a consultant.

We've calculated your savings, and we estimate that you will save over 90% compared to the cost of a lawyer or consultant. In other words, you'll save thousands of pounds – with no drop in quality!

FREE ONE ON ONE CONSULTATION WITH A GDPR EXPERT

IS GDPR CREATING MORE QUESTIONS THAN ANSWERS?

The Business Train are offering a limited number of free consultations with a GDPR consultant to provide you with the clarification you need to make sure that your business is compliant with the new regulations.

If your journey has created more questions than answers or if you'd like to make sure your changes are adequate, we can help.

The Business Train has already worked with over 50 companies to get them moving towards full compliance, from a sole trader to a large corporate. This is an invaluable investment of time for any company, large or small, affected by the GDPR.

This offer is extremely limited and we recommend early application to avoid disappointment. Now that the GDPR requirements can be enforced, can you afford not to act?

CONTACT US TODAY

Even though it might seem overwhelming with all of these policies, you really can implement GDPR by yourself.

All you need is to purchase one of our documentation toolkits. Our toolkits and other resources were developed for ease of use and to be understandable, with no expert knowledge required.

alan@thebusinesstrain.co.uk

Direct mobile 07764 291731
Switchboard 0203 633 1967