GDPR Basics

Inform.
Transform.
Protect.

VENOM·IT

GDPR Basics

Welcome

In this booklet, we aim to explain the basics of the GDPR in a way that is more easily digestible and, hopefully, made practical and useful for employees, managers and business owners alike.

Remember that the middle two letters of GDPR stand for Data Protection—this means taking proper cyber-security measures. Probably 50% of GDPR compliance relies on healthy IT systems, and the other half is split between legalities such as privacy notices and contracts, and organisational measures such as staff training and assigning of data access privileges. If you can prevent a data breach from happening in the first place, you've done well. Enjoy the booklet!

GDPR is an important regulation that is designed to protect the rights of all European Union and UK subjects' data. It clarifies what companies that process data must do to safeguard these rights. Making sure your business complies with the GDPR is crucial and Venom is here every step of the way to help you make that happen.

The GDPR – why you should pay attention

The GDPR (General Data Protection Regulation) outlines measures an organisation must take when handling personal data.

It came into effect on the 25th of May 2018. The UK DPA 2018 is a similar set of legislation that adopts the GDPR as UK law, with a few small amendments and additions.

Think of the GDPR as health and safety for computers. We might not always like it, but ultimately it is there for our protection.[1] Here are some highlights of these new laws you should be aware of, with emphasis on what business owners and managers should know.

Please bear in mind that this is not an exhaustive list, and by no means a source for legal reference. However, as professionals responsible for helping our clients meet key aspects of GDPR, we want to help you get a better understanding of your duties – some of which could be completely new to many business owners and managers. It remains your responsibility to make sure you know the law and comply with it.

In order to make it easier to read, certain liberties were taken with the exact wording – for example, 'data controller' has been replaced with 'you' or 'your company', and 'data subject' has been replaced with 'customer', 'people' or the like. For this reason, there is a fairly comprehensive reference section at the back, where you can read the exact 'letter of the law'.

Does the GDPR apply to me?

Absolutely. All types of organisations are included in the GDPR – from micro to massive.[2]

However, the GDPR covers your professional and/or commercial activity only – anything unconnected to this falls outside of its remit.

This means it doesn't cover you keeping a personal record of addresses unrelated to your business, or sharing unrelated information during personal social networking.[3] That being said, the providers of social networking platforms have to comply with the GDPR.

Cyber security providers such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) will often have legitimate access to computer networks containing personal data during the course of their work (i.e. you're not breaking GDPR rules by letting them in). These teams will sometimes have to access this information to prevent unauthorised access, stop DoS attacks or the spread of malware, but only to the extent that is strictly necessary to ensure the safety of the computer network.[4]

The GDPR does not apply to matters of national security,[5] nor does it apply to the investigation and prosecution of criminal offences, although the police and everyone else still have to apply the same rules to their own organisation.[6]

The rules say that public authorities such as tax and customs authorities, financial investigation units and independent administrative authorities are allowed to request personal data, but these requests should always be in writing with reasons given.[7]

Practically speaking, this means that if you were to get a phone call from someone claiming to be from HMRC who wants access to the personal data of some or all of your customers/employees, it will most likely be a scam.

You will be relieved to know that the GDPR does not apply to the deceased.[8]

Additional legislation that may apply to your organisation

In the UK, the GDPR has been incorporated into the Data Protection Act of 2018 (aka UK DPA 2018), with a few additions and amendments.

You should also be aware of the Privacy and Electronic Communications Regulation (PECR), which applies to the sending of electronic marketing messages (by phone, fax, email or text), use of cookies, or provision of electronic communication services to the public.

What will happen if I don't comply?

For the first time ever, businesses can face fines in the millions, rather than the thousands, for a lack of proper data security measures [9].

Negligence and non-compliance to accepted standards are now factored into the punitive decision-making process, and can result in significant financial penalties. In addition, jail sentences are a real possibility in the worst cases of malicious intent or reckless disregard:[10]

- You could face fines for infringements of the GDPR, not just data breaches,[11] with fines ranging from 2-4% of revenue.[12]
- Your customers could seek compensation against you if their rights have been infringed.[13]
- You could be ordered to compensate any person who suffered damage due to your processing their personal data in a manner that infringes the GDPR.[14]
- You could also face criminal charges for infringements of the GDPR.[15]

Apart from the financial implications, the damage to your organisation's reputation could be catastrophic, with potential customers unwilling to trust you with their personal data. It is therefore vital that you have a sensible plan in place to protect your data from cyber threats.

Top tip…

Be careful when installing new mobile apps—take the time to read through the permissions and deny anything that looks suspicious (e.g. a game wanting access to your address book or calendar).

The Six Principles of Privacy

The GDPR has summarised its many requirements into six data protection principles. It also provides resources for those businesses who want to know how they can achieve compliance.

1. Lawfulness, Fairness and Transparency

This principle more or less speaks for itself. You need to make sure your data collection practices don't break the law and don't hide anything from data subjects (i.e. the people about whom you're collecting data).

2. Limitation of Purpose

You should only collect personal data for a specific purpose, clearly state what that purpose is and only collect data for as long as is necessary to complete that purpose. More freedom is given to data processing related to archiving in the public interest, or for scientific, historical or statistical purposes.

3. Data Minimisation

You must only process the personal data you need to achieve your stated purpose. There are two good reasons why this is important. Firstly, if there is a data breach then it limits the amount of data exposed. Secondly, it makes it easier to keep your data accurate and up-to-date.

4. Accuracy

The accuracy of personal data is absolutely central to data protection. According to the GDPR, every reasonable step must be taken to erase or rectify data that is incomplete or inaccurate. Individuals have the right to request that you do so within 30 days.

5. Limitation of Storage

Don't keep personal data that you don't need. Depending on your industry, the length of time you need to store data might vary. If you're unsure in any way about how long you should be keeping it, consult a legal professional. Nevertheless, you should periodically review and erasure the data you no longer require.

6. Integrity and Confidentiality

This relates explicitly to protecting your data. The GDPR does not define exactly which steps you need to take, because technological and organisational best practices continue to evolve. Nevertheless, it says personal data must be:

"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".

Did you know?

A common mistake in larger companies, is a file & data structure that's far too lenient - too many people have too much access to too much data.

What types of data fall under the GDPR?

Still use a Rolodex? The GDPR covers electronically-kept as well as manually-kept personal data, so it doesn't matter what storage techniques you use.[16]

Things such as IP addresses, computer cookies and RFID tags could constitute personal data if they can be used to identify someone, either alone or along with other information.[19]

Genetic data is also considered personal data.[20]

As you would expect, all information pertaining to health status is considered sensitive personal data [21]. This includes information relating to someone's past, current or future physical or mental health status, as well as any disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state.

The GDPR does not apply to anonymous information.[22] This puts using pseudonyms in bit of a grey area, with the main concern being the ease or difficulty with which a person can be identified or singled out in spite of using a pseudonym.

Pseudonyms may be used to reduce the risks associated with the storage of personal data [23], but that doesn't exempt you from complying with all the other GDPR criteria.

The GDPR also applies to personal data gathered for scientific,[24] statistical [25] and historical purposes.[26]

There is also a distinction between personal data and special categories of data, or sensitive data.[29] With a few exceptions made for legal purposes, public interest/ public health, health care, non-profits with religious, political or philosophical aims and trade unions, you may not process the following data:[30]

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life or sexual orientation

We subcontract our data processing – do we need to do anything?

Yes. When outsourcing data processing, the onus rests on you to make sure that the subcontractor is GDPR-compliant. [31]

The good news is that the certificates and/or approved codes of conduct of the sub-contractor can be used by you as proof (or part of your proof) of your own GDPR compliance.

When outsourcing data processing to non-EU countries, the GDPR still applies and must be enforced on all sub-contractors.[32]

Data processors from outside of the EU should adhere to the GDPR when processing data of people within the EU – this is especially true for internet data processing techniques to profile a person and predict her or his personal preferences, behaviour and attitude.[33]

Lawful Basis and Consent

You have to have a valid, lawfully justifiable reason for collecting someone's data.

The GDPR recognises the following bases:

- Contractual Obligation
- Legitimate Interests
- Consent
- Legal Obligation
- Vital Interest
- Public Interest

Here's a quick illustration of what we mean:

Someone is sending you a parcel. The delivery company asks for your address (Contractual Obligation—they can't deliver your parcel if they don't know where) and your phone number (Legitimate Interest— to call you in case you're not home to arrange a different delivery date).

They also ask for your email address to send you a monthly newsletter (Consent—this falls under marketing and you have the right to opt in or out). You agree at first, but later ask the delivery company to remove your name from their database (Right to be Forgotten) but they only remove your name from the marketing list. They have to keep business and transactional records for 7 years (Legal Obligation).

Unfortunately, your parcel went on the same truck as a consignment of weed killer that had leaked. The parcel delivery company gives your details to the company that makes the weed killer, who then call you with an urgent warning and safety instructions (Vital Interest).

Lastly, the authorities step in. From the delivery company they get the names and contact details of any individuals and companies who might have been affected, and issue further warnings and safety instructions (Public Interest).

Top tip...

Make sure you have proper consent before sending mass marketing emails. Historically, the ICO has written numerous fines for non-compliant marketing.

How does consent work?

Before acquiring consent, it's worth double-checking that you can't perhaps rather use 'contractual obligation' or 'legitimate interest' as your lawful basis for processing their data

Unless you have a different lawful basis, you need their consent. Not only that, but the act of giving consent must be clear, affirmative, specific, freely given and unambiguous.

Consent does not count as 'freely given' if the person has no genuine or free choice about giving it. Neither does it count if they are unable to refuse or withdraw consent without negative consequences.[35]

For that reason, consent is also only valid if the customer can withdraw it at any time [36]

And if the customer is under 16, you need two things: You need parental consent to process their personal data, and you also need to verify that the consent came from the parent and not the child.[37]

A customer can give their consent electronically or verbally and it could include ticking a box or choosing settings. However, silence, pre-ticked boxes and inactivity do not constitute consent.

You need identify who the data controller is (i.e. the company that will be using the data) and explain each purpose for which their data is being collected – your customer needs to consent to them individually.

Requests for consent should not be unnecessarily disruptive and you need to be able to demonstrate that consent was given [38].

In addition, the declaration of consent must have clear terms and be written in plain language, with no unfair terms [39].

You also may not use their data for other reasons, unless additional consent has been obtained from the customer [43]

How should data be processed?

We've covered a lot of the principles behind data processing, but there are still some things you need to remember as the custodian of other people's personal data.

Being the custodian carries certain risks, and you need to these out when collecting people's data, along with any rules, safeguards and rights associated with the data collection

You also need to make sure that your data processing procedures protect your customers (data subjects) against:[45]

- Physical, material or non-material damage
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality of personal data
- Unauthorised reversal of pseudonymisation
- Any other significant economic or social disadvantage

Another thing to keep in mind is that you should not use exclusively automated processes to determine the outcome of customer applications (e.g. credit applications).[46] Customers have the right to obtain human intervention, to express their point of view, and to obtain an explanation

What responsibilities do companies have?

If you haven't done so already, your first move should be to subscribe to a GDPR code of conduct.

It should cover topics we have included in here as a cost-effective way of ensuring compliance. In addition (or as an alternative) you should obtain a certification of adherence to the GDPR47. Or if there is no formal GDPR certification, obtain other well-recognised certificates such as Cyber Essentials, ISO 27000 family of certification, CSA STAR and others.

However, you may also be required to appoint a data protection officer if your core activities consist of data processing operations, you process data on a large scale or from the special categories (Sensitive Data) or criminal convictions [48].

You should be able to proactively prove your compliance with the GDPR regulations.[49] This means proving that you have implemented the appropriate technical and organisational measures, along with internal policies, to demonstrate compliance to the new legislation.[50] As mentioned earlier, the certificates and code of conduct mechanisms used by a sub-contractor who handles your data processing for you, also count towards demonstrating your own compliance.

Your staff need to be educated both on GDPR as well as cyber security, with at least annual refresher training, all of which needs to be documented.

People have a right to know what information you have about them, but you should take all reasonable measures to verify the identity of the person requesting the personal data.[51]

You should maintain records of data processing activities, as the supervising authorities may ask you for these records as proof of your compliance.[52] You should also keep a suppression list of people who have opted out from marketing communications.

Any public communications or communications aimed directly at the customer should be clear and concise, easily accessible and easy to understand, with visualisations whenever appropriate, especially where children are the data subjects.[53]

If you're going to process a large amount of personal data, affecting a large number of data subjects, you should do a risk assessment and implement systems to mitigate those risks to prevent data processing infringements.[54]

Your risk assessment should consider:

- The appropriate level of security
- Confidentiality
- Costs of implementation in relation to the risks
- The nature of the personal data to be protected
- Accidental or unlawful destruction, loss, alteration, unauthorised disclosure

Where a high risk is established, you should carry out an additional data protection impact assessment.[55] This applies in particular to large-scale data processing operations [56] (processing data at a regional, national or supranational level), which should do such risk and impact assessments prior to commencing processing.[57]

An exception to this rule is if you are working as an individual physician, other health care professional or lawyer.[58]

Auditing and audit trails are an integral part of GDPR compliance and ISO compliance, which means you should have a policy and procedures for authentication and access control of your premises, as well as your IT systems.

You should also have certain documentation in place in order to show your compliance. This would include at least the following:

1. Data Protection Policy
2. Acceptable Use Policy
3. Access Control Policy
4. Antimalware Policy
5. Cloud Computing Policy
6. Cryptographic Policy
7. Electronic Communications Email and Internet Policy
8. GDPR Controller/Processor Agreement Policy
9. Information Security Policy
10. Mobile Device Policy
11. Network Security Policy
12. Records Retention and Protection Policy
13. Physical Security Policy
14. Privacy Policy
15. Website Privacy Policy
16. DPIA (Data Protection Impact Assessments) scope and procedure
17. SAR (Subject Access Requests) procedure

Did you know?

53% of all crimes reported in the UK are computer-related? Cyber security is becoming more important than ever before. Stay safe!

Controller or Processor?

You are the data controller if…

You determine the purposes and means of the processing of personal data. This could be as a person or an organisation and you could also have joint responsibility with another person or organisation.

Simply put, if it was your idea to gather and use the data, whether you did it yourself or got someone else to do it, you're the data controller

- ASK YOURSELF: In which areas does your organisation act as a controller?

You are the data processor if…

You are processing personal data on behalf of the controller.

Simply put, if you are processing data at somebody else's behest, you're the processor

- ASK YOURSELF: In which areas does your organisation act as a processor?

As controller, an important part of your responsibly is to ensure that all of your processors be vetted and bound by standard contractual clauses (SCCs), which are a simple way to ensure that contracts between controllers and processors comply with the GDPR. Each processor must have a contract in place that includes these standard clauses in addition to your service agreement.

Top tip...

Configure remote data wiping on your mobile devices to prevent your data from ending up in the wrong hands if ever your device gets lost or stolen.

Can I use customer data for marketing?

Yes, but only if you have obtained consent or where there is an existing relationship between you and the customer.[59] You should also remember that the customer or prospect has the right to object to you using their data for this purpose, and they should expressly be made aware of this right.[60]

As part of your responsibility to the people on your database, you should provide means by which they can easily request and obtain, access, rectify or erase their personal data – including medical records.

Not only that, but customers need to be able to obtain their records at no charge, and in a commonly used machine readable format[62]

What rights do customers now have?

People have the 'right to be forgotten' – which means you may not keep any personal data about someone after they have requested to have their data erased.[64] This also means that if that data has been made public, you need to delete any links to, copies or replications.[65]

However, this is not an absolute right – certain overriding rules of retention often apply, such as HMRC requirements, or retention of medical and criminal records, to which different sets of rules apply.

Lastly, the 'right to be forgotten' does not actually mean forgetting that person – you have to move them to a suppression list, keeping only enough details to identify them in future as e.g. having opted out from marketing.

Children have special protection of their personal data and you need parental consent to process children's data. However, in the case of preventative or counselling services offered directly to the child, parental consent may not be necessary.[66]

As we've already pointed out, special care must be taken when handling sensitive personal data, such as:[67]

- Racial or ethnic origin
- Political opinions
- Religion or philosophical beliefs
- Trade union membership
- Genetic data
- Data concerning health
- Data concerning sex life
- Criminal convictions and offences or related security measures
- Where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour
- Location or movements
- Personal data of vulnerable natural persons, in particular that of children
- Cases where processing involves a large amount of personal data and affects a large number of data subjects

Did you know?

An advanced or next-gen Firewall has a faster Internet speed limit than a basic Firewall.

What are our rights as an organisation?

You have the right to bring an action of annulment before the Court of Justice, should you be dissatisfied with the outcome of an investigation and subsequent decisions.[68]

A group of companies or institutions that are affiliated to a central body, may share personal data within the group.[69]

Supervising Authority

In the UK, the ICO has been appointed as the supervising authority to uphold GDPR legislation. You can contact* the ICO to:

Raise concerns about violations of privacy laws such as the GDPR or PECR

Get further information on privacy laws

Report data breaches

https://ico.org.uk
0303 123 1113 (UK)*
016 2554 5297 (Welsh)*
+44 1625 545 700 (International)*

*"Before you call or email [the ICO]...please make sure you have searched [the ICO] website for all relevant guidance. "

Top tip...

Learn how to spot fake emails.
41% of all people can't.

What happens if there is a data breach of some sort?

Should a data breach occur, you have a responsibility to report it to the supervising authority within 72 hours.[70] You also have an obligation to let your affected customer know about the data breach, so that she or he can take the necessary precautions.[71] The supervisory authority may choose to bring in an intervention [72] and you may be required to submit to a data protection audit [73]

Having said that, in the UK not all data breaches have to be reported to the ICO – there is an assessment tool on their website that can help you determine whether or not to report the matter, found here: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

You should however, not delay in completing the assessment, and should also consider whether or not to notify your customers of the breach whether reporting to the ICO was required or not.

Handy Additional Checklist

- Does your website have an SSL certificate?
- Do you have a privacy policy, and is it available on your website?
- Do you have an explicit opt-in for people to receive marketing communications?
- When you send marketing material, is there a clear opt-out or unsubscribe button near the end of each email?
- When doing telemarketing, check both the private and business TPS lists first.

Definitions

Excerpts taken from Article 4 of the GDPR:

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.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processing 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51.

Top tip...

Secure your phone and tablet with reputable antivirus software—mobile fraud rose 24% in 2018 with 150 million attacks during the first 6 month alone.

Reference Section

1 One of the main aims of the GDPR is "…the protection of natural persons in relation to the processing of personal data"

2 **Recital 13** of the GDPR states, in part: "Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors"

3 **Recital 18** of the GDPR states, in part: "This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity… household activities could include correspondence and the holding of addresses, or social networking"

4 **Recital 49** of the GDPR states, in its entirety: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

5 **Recital 16** of the GDPR states, in part: "This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security"

6 **Recital 19** of the GDPR states, in part: "with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes.

7 **Recital 26** of the GDPR states, in part: "The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing"

8 **Recital 27** of the GDPR states, in its entirety: "This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons."

9 **Article 5** of the GDPR says, in part: "Personal data shall be 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 ('integrity and confidentiality')"

10 **Article 83** of the GDPR says, in part: "When deciding whether to impose an administrative fine and deciding on the amount… due regard shall be given to…the intentional or negligent character of the infringement… [and] adherence to approved codes of conduct… or approved certification mechanisms…"

11 **Recital 150** of the GDPR states, in part: "…each supervisory authority should have the power to impose administrative fines"

12 **Article 83** of the GDPR states, in part: "Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4). 4.5.2016 L 119/82 Official Journal of the European Union EN 5.Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). 6.Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"

13 **Recital 142** of the GDPR states, in part: "Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association … to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects"

14 **Recital 146** of the GDPR states, in part: "The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage"

15 **Recital 149** of the GDPR states, in part: "Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation"

16 **Recital 15** of the GDPR states, in part: "The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing"

17 **Recital 1** of the GDPR states, in part: "…processing of personal data is a fundamental right… everyone has the right to the protection of personal data concerning him or her"

18 **Recital 6** of the GDPR states, in part: "a high level of the protection of personal data"

19 **Recital 26** of the GDPR states, in part: "….online identifiers provided by … devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them"

20 **Recital 34** of the GDPR states, in part: "Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample"

21 **Recital 35** of the GDPR states, in part: "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information … collected in the course of the registration for, or the provision of, health care services … a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

Top tip…

Public Wi-Fi is notoriously unsecured—use your own mobile data wherever possible.

22 **Recital 26** of the GDPR states, in part: "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly… account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"

23 **Recital 27** of the GDPR states, in its entirety: "The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection."

24 **Recital 159** of the GDPR states, in part: "Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing"

25 **Recital 162** of the GDPR states, in part: "Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality"

26 **Recital 160** of the GDPR states, in part: "Where personal data are processed for historical research purposes, this Regulation should also apply to that processing"

27 **Recital 53** of the GDPR states, in part: "Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy."

28 **Recital 51** of the GDPR states, in part: "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin… Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms."

29 **Recital 10** of the GDPR states, in part: "Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data')"

30 **Article 9** of the GDPR says, in part: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

31 **Recital 81** of the GDPR states, in part: "To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act"

32 **Recital 22** of the GDPR states, in part: "Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union"

33 **Recital 24** of the GDPR states, in its entirety: "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

34 **Recital 32** of the GDPR states, in its entirety: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

35 **Recital 42** of the GDPR states, in part: "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

36 **Article 7** of the GDPR states, in part: "The data subject shall have the right to withdraw his or her consent at any time"

37 **Article 8** of the GDPR states, in part: "Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child… The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child"

38 **Recital 42** of the GDPR states, in part: "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation"

39 **Recital 42** of the GDPR states, in part: "a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended"

40 **Recital 39** of the GDPR states, in its entirety: "Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

41 **Recital 40** of the GDPR states, in part: "In order for processing to be lawful, personal data should be processed on the basis of the consent...or some other legitimate basis, laid down by law."

Top tip…

Perform a review of your user access rights every 6-12 months. You'd be surprised at what you sometimes find!

42 **Article 5** of the GDPR states, in part: "Data shall be… processed lawfully, fairly and in a transparent manner… collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… adequate, relevant and limited to what is necessary… accurate and, where necessary, kept up to date… 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… 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 ('integrity and confidentiality')"

43 **Article 14** of the GDPR states, in part: "Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information"

44 **Recital 61** of the GDPR states, in part: "The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case."

45 **Recital 75** of the GDPR states, in its entirety: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

46 **Recital 71** of the GDPR states, in part: "The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her… In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."

47 **Articles 40** and 42 of the GDPR state, in part: "The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises… The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation"

48 **Article 37** of the GDPR states, in part: "The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences"

49 **Recital 74** of the GDPR states, in part: "…the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures"

50 **Recital 71** of the GDPR states, in part: "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default."

51 **Recital 64** of the GDPR states, in part: "The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers"

52 **Recital 82** of the GDPR states, in its entirety: "In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations."

53 **Recital 58** of the GDPR states, in part: "any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used"

54 **Recital 83** of the GDPR states, in its entirety: "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."

55 **Recital 84** of the GDPR states, in part: "In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk"

56 **Recital 91** of the GDPR states, in part: "This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk"

57 **Recital 90** of the GDPR states, in part: "…a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk"

58 **Recital 91** of the GDPR states, in part: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory"

59 **Recital 47** of the GDPR states, in part: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller... The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

60 **Recital 70** of the GDPR states, in its entirety: "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information."

Did you know?

There were 1013 data breaches in the USA in 2016. By comparison, the U.K. had only 38 breaches. Where you store your data does matter.

61 **Recital 59** of the GDPR states, in part: "Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means"

62 **Article 20** of the GDPR states, in part: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format"

63 **Recital 63** of the GDPR states, in part: "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records"

64 **Recital 65** of the GDPR states, in part: "A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed"

65 **Recital 66** of the GDPR states, in part: "To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data"

66 **Recital 38** of the GDPR states, in its entirety: "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

67 ibid

68 **Recital 143** of the GDPR states, in part: "Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice… Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them"

69 **Recital 48** of the GDPR states, in its entirety: "Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."

70 **Recital 85** of the GDPR states, in part: "…as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it"

71 **Recital 85** of the GDPR states, in part: "The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions"

72 **Recital 87** of the GDPR states, in part: "Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation"

73 **Article 58** of the GDPR states, in part: "Each supervisory authority shall have all of the following investigative powers… to carry out investigations in the form of data protection audits… to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law"

Make sure your business is GDPR compliant, the Venom team are here to help you make that happen.

Get in touch

Please contact us if you'd like to discuss any of the information outlined in this document

0330 202 0220
sales@venomit.com

Did you know?

An advanced Firewall scans the traffic for malicious content, detects & blocks attempted intrusions (hackers), and gives you full control of each user's access rights. A good firewall is your first line of defence.

More top tips

Top tips…

- Get Cyber Essentials Certified. It's a great way of checking both real-world and digital security measures, and having the certification makes your organisation more appealing as a partner.
- A cloud-hosted virtual desktop, such as the ones provided by Venom IT, is a very secure and convenient way of working remotely, and counts towards GDPR compliance by virtue of being ISO 27001-certified.
- A degree of technological monitoring and control… balanced with age-appropriate education and guidance throughout their childhood – will show your children you care and go a long way towards keeping their digital lives safe and happy.
- Get a specialist cyber security company like Venom IT to perform a network audit at your organisation to ensure all your devices and systems are secure.
- Choose a business-grade email provider (rather than a freebie) that can check incoming emails for spam, malicious links and viruses, and 'sandbox' attachments to make sure that they are safe.
- Download and read Venom IT's easy-to-understand companion booklet entitled Cyber Security Basics Every Business Owner Should Know

Did you know?

- Switching to cloud-hosted desktops and/or servers, you could gain access to top-end security without having to bear the huge costs normally associated with such high-end equipment.
- Windows XP is no longer considered fit for use in business. Upgrade to the latest version of Windows for better security. Venom IT offers free Windows upgrades on all our cloud-hosted desktops.
- In 2015, around 4000 infected apps were identified on the Apple App store and in 2017 around 800 infected apps were found on Play Store? The point is, less is more—fewer apps on your phone = better security.
- ISO 9001 and ISO 27001 count towards GDPR compliance? The good news is, if you don't have ISO 27001, storing your data with an ISO 27001-certified Cloud provider also counts towards your compliance.
- The average age of cyber criminals is 17 – children need to be taught what's right & wrong, especially when it comes to the world of computers.
- Worldwide, over the past 5 years more than 5,000,000 organisations achieved ISO9001 certification, but fewer than 150,000 (3%) achieved ISO27001 certification. Venom IT is one of them!
- Venom IT runs 24/7 virus scanning on all its data centres? This means a much higher level of protection for your data than what is ordinarily available on an on-premises server.
- There are around 6.4 billion fake emails sent worldwide every day!
- Venom IT is partnered with Microsoft, Fortinet, Veeam, Citrix, Webroot, 3CX and others. Our aim is to supply you with best-of-industry services that are tailor-made to suit your business, coupled with competitive pricing.

GDPR Basics

venomit.com

Please contact us if you'd like to discuss any of the information outlined in this handbook

0330 202 0220
sales@venomit.com

VENOM·IT