DVV solutions

YOU'RE ONLY AS STRONG AS YOUR WEAKEST LINK

GDPR & THIRD PARTY RISK

QUICK GUIDE

GDPR – Resistance is Futile

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations approach the privacy, security and use of Personally Identifiable Information (PII).

Not GDPR Ready? You're Not Alone

- A June 2017 survey carried out by the Direct Marketing Association found that only **54% of businesses expect to be compliant** by the deadline.
- **Only 2%** of organisations stating they are "GDPR-ready" **are actually fully compliant**, according to a Veritas study in July 2017
- **71% of UK businesses are unaware of fines under the GDPR** and a number of them fear they would go out of business if forced to pay the maximum. (YouGov, May 2017)

GDPR represents a huge change (and opportunity) for all businesses. Whilst specifics around rules and implementation remain unclear, three things are certain: -

! GDPR is coming on May 25th 2018
– not even Brexit will save you!

! The potential penalties for a breach are severe
– up to €20m or 4% of global revenue, whichever is greater

! Delegating data processing does not delegate liability
– You can be held jointly liable for a breach of a Third Party supplier

It's Not All Doom and Gloom

GDPR should be seen as a blessing in disguise. GDPR will encourage us to build more meaningful relationships with clients and prospects, which is in everyone's interests.

No more spamming, no more cold calling, no more irrelevant emails sent or received means **more relevant content**, **more engaged customers** and an **increased focus on security and privacy** of all our personal data.

So how can we make sure GDPR is a Win-Win for Data Controllers and Data Subjects alike?

Establishing a Clear Strategy and Ownership

In May 2017, the ICO issued a briefing document on the **"12 Steps to Take Now"** in preparing for GDPR. We certainly recommend this as a basis from which to build your compliance, but starting at the very beginning it is essential to understand where you are today and ensure a solid structure from which to work from: -

- √ **Clearly define the roles and responsibilities for GDPR compliance.**
  Whether it's a working group or designated Data Protection Officer, identify some experts then train and support them.

- √ **Scope and document all the data and storage platforms you possess.**
  Create a data register and record all the internal and external processes, policies and platforms that support it.

- √ **Review and define clear policies, workflows and actions.**
  For example, in the event of an internal breach, external security incident, a complaint or request for access who is responsible for doing what?

- √ **Collate and review all your contracts with Third Party suppliers.**
  Do they include the right to audit? Do they directly reference compliance with GDPR or any other regulatory requirements? How well do they cover GDPR-compliant data processing and data security controls?

Remember, GDPR applies just as much to employee PII data as it does anyone else. It's just as important to ensure internal and outsourced functions and processes surrounding your employee data are managed with the same level of due diligence.

Likewise, departments such as HR and Finance need to be given a seat at the table when planning your GDPR compliance strategy and deployment.

Turning Compliance Pain into Commercial Gain

Regulatory compliance can be seen by some as an onerous, box-ticking exercise. But there is no way out of it. We suggest this time and effort is used wisely to refresh your approach to the acquisition, usage and storage of data and turn it into a competitive advantage.

There are a few simple principles behind GDPR that seek to provide a greater level of security and privacy for each individual employee or customer. These offer a guide as to the key considerations you need to start planning for and building teams and processes to execute as you prepare for GDPR compliance.

As you will see overleaf, for every issue and change you need to address for GDPR there is a valid commercial opportunity to improve your data governance, operational efficiency and sales and marketing efforts.

	The Impact	The Opportunity
Gaining specific and explicit consent to store and use data	Gone will be the days of "opting-out". People must have to clearly "opt-in" and your clients and prospective clients are going to be telling you exactly how you can use their data. Providing detailed terms of use and offering choices over whether you can process, share and use their data will be an essential part of gaining consent.	Improve the quality and process of data collection. Understand the contact and profile data you need, why and what you use it for. Become more effective in collecting new contacts and gaining trust and buy-in to send relevant information to engaged audiences.
Fair and transparent processing	You can no longer contact people without their explicit consent, or share and use their data without their prior approval.	Think about how your data strategy adds value to your Customers. Can you delivering a better Customer experience? Are there better ways of engaging each audience or individual? How can you be more targeted and focused in your communications to make campaigns and messaging more successful?
Limiting data to what is relevant and necessary	Any personal data you hold must be kept to the bare minimum and you'll have to keep robust records to demonstrate your efforts to remain compliant. The way in which you approach contacts and the amount of data you request and store is going to have to be innovative and incisive.	Use GDPR as the chance to refresh and purify your databases. Focus on the data that is really critical to making your business tick and use it in more intelligent ways to create new opportunities with Customers and Prospects.
Keeping records accurate and for no longer than is necessary	It is your responsibility as the data controller to ensure good housekeeping of PII data and to retain records for no longer than is necessary. You should review and record your existing practices and policies and look at how valid and accurate your current data is.	You now have a great reason to contact Customers and Prospects. Reach out to cleanse and update their data, illustrate good diligence and understand what products, services and issues are most relevant to them.
Individual's rights to request, erasure, rectification or restriction of data	You'll need to develop, document and implement processes that ensure the rights of the individual to access their data or even be forgotten are met. Address how simple and easy it could or should be for individuals to access, update and manage their profile and subscriptions.	Become more responsive, transparent and customer-friendly in the way in which you offer and deliver these rights. You may also identify ways to improve efficiencies in the storage and access of data.
Ensuring appropriate security of data	If you have a breach, you can be fined up to 20 million Euros or 4% of group worldwide turnover (whichever is greater). You'll need to ensure any outsourced partners that process or store your data are delivering levels of security that make them AND you GDPR compliant.	Put robust and auditable systems and controls in place to protect some of the most mission-critical information your business owns. Are you working with the most secure, reliable suppliers? Can your security and diligence create a differentiator as the trusted custodian of Customer data?
Nested liability with Third Parties	As Data Controller, you must ensure the due diligence and security practices of any "data processors" you share PII data with – such as an outsourced agency for Email or Telemarketing, Payroll or Payment services. And crucially YOU assume joint responsibility for what happens to it. This means that YOU can be held liable if one of your Third Parties gets breached as a result of them failing to meet GDPR requirements.	Apply (and prove) greater due diligence to your choice of Third Party suppliers and review your outsourcing practices and programs. Are they GDPR compliant? How can they prove it? How do existing suppliers stack up against others in their field? Can operational efficiencies be improved? Are you effectively monitoring emerging threats in the data supply chain?

The Sooner you Start…..

With less than a year to go, most organisations will need to go through some significant effort and changes — and there's no time to lose. Like any big task you'll need to take it step by step. We suggest you:

PRIORITISE BASED ON RISK	You will need to prioritise actions that address the highest risks to the business if left unchecked. These priorities will be different for each organisation in line with your strengths and weaknesses and levels of data security. But you may want to focus on the business processes and operations where you are not in complete control.
CONSIDER TIME TO EXECUTE	Take into account how long each action will take to complete. Reviewing and renegotiating contracts can be a lengthy process and auditing and assessing supplier security controls doesn't happen overnight. It would perhaps be foolish therefore to spend the majority of your time and resource strengthening internal security at the expense of unknown external risks from Third Party relationships.
BE HONEST, NEED HELP? GET HELP	Finally, be realistic and maybe even critical of your current position. It is better to be over prepared than under prepared. And when in doubt, seek professional counseling. This is where DVV Solutions can help you in the transition to complete GDPR compliance.

You're only as Strong as your Weakest Link

DVV Solutions have developed a series of simple and straightforward GDPR Third Party risk assessments to help you understand your suppliers' (and therefore YOUR) current levels of compliance with GDPR and continuously monitor the threat landscape.

By streamlining your efforts using GDPR-specific questionnaire templates, whilst allowing tailored questions to be asked, you will increase the likelihood of receiving clear and well documented answers that accurately reflect each Third Party's capacity to comply with GDPR and your own security controls. Our team of certified Risk Assessors can also recommend and help action remediation plans to mitigate any risks to your data security and privacy.

We'd be pleased to hear from you and help find the most cost-effective way to achieve full GDPR compliance throughout your data supply chain.

Call us: **+44 (0) 161 476 8700**

Visit us: **dvvs.co.uk**

Visit the ICO: **ico.org.uk/for-organisations/data-protection-reform**