Deeson.

The only GDPR guide you'll enjoy reading

A collaborative white paper
by leading UK digital agencies

About Deeson

Deeson is a digital agency delivering high profile, high stakes digital transformation projects for clients including Johnson & Johnson, Robbie Williams, ITV, and National Crime Agency.

We've developed a reputation for delivering complex projects through our integrated approach to strategy, engineering, design and user experience.

Take a look at some of our recent work at http://deeson.co.uk/about.

About this guide

With only a few months to go before the General Data Protection Regulation (GDPR) becomes enforceable across Europe, now is the time to begin your implementation process. This guide will help you to devise your strategy for GDPR adoption across all levels of your business.

As a digital agency serving enterprise clients across diverse sectors as well as international borders, we have had to take a long hard look at our own processes, both internally and externally, to find the right way forward for ourselves.

This guide shares part of the journey we have taken to make sure we are on the right track. It is not designed to be an authoritative instruction manual, nor is it legal advice. It is, however, part of our commitment to protect our customers and clients. We are happy to share what we have learned with you.

We have taken a very different view of GDPR compliance, and we want to explain why that matters.

Background

When GDPR's final form began to take shape in 2015, we thought its provisions were a straightforward upgrade to an outdated law: a cumbersome but necessary process to bring 1995's data protection rules out of the dial-up era and into the cloud. We were aware that people were losing trust in businesses due to today's growing privacy concerns, and saw GDPR as an opportunity to put that right.

There was an ulterior motive too. We knew that a lack of regard for data protection meant that many fellow digital professionals, both friends and rivals, were surprisingly unaware of their legal and moral obligations. So we were glad that GDPR would bring issues to the forefront which we had been advising clients on for quite some time.

In hindsight, our perspective from 2015 was the product of a very different time. In two short years, the data protection and privacy landscape, and the world we work in as digital professionals, has changed beyond all recognition.

We feel that we have a role to play in safeguarding the people who use the services we build. GDPR compliance is a part of that. In a world where data gives unprecedented power to organisations – whether national, corporate, political, charitable or 'other' – we no longer look at data protection as solely a matter of legal compliance. We view it as an an act of social responsibility, user protection, and quite possibly, as a safeguard against what may be to come.

You have a role to play as well. This guide will explain what you need to know.

What does this affect?

GDPR replaces the existing data protection regime, 1995's Data Protection Directive. In the UK we know it as the Data Protection Act of 1998.

GDPR, and the EU's principles of data protection and privacy in general, pertain to **personal data**.

Personal data, for our purposes, means information about a living individual who could be identified from that data, either on its own or when combined with other information. GDPR officially defines personal data as "any information relating to an identified or identifiable natural person."

Your customer records, and the data that people generate using or accessing your services, are personal data.

Beyond personal data there is also **sensitive personal data**, which is defined as any information concerning an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

Sensitive personal data requires stricter curation, and the loss or breaches of such data rightfully carries stricter punishments.

GDPR **expands the definition of personal data** from the 1995 standard to include an individual's:

- Genetic data
- Biometric data
- Location data
- Online identifiers

The latter definition, online identifiers, is critical to digital businesses. Any information created through interaction with a site, app, wearable, or online service which could identify the individual – whether that is an analytics record, a check-in map, a health tracker, or the information exchanged through a social media login – is personal data. That data may well also be sensitive.

The 1995 data protection principles established that personal data must be:

- Processed in a manner which is fair and lawful;
- Used only for the manner in which it was intended to be used;
- Processed in a manner which is adequate, relevant, and not excessive;
- Accurate and kept up to date;
- Not kept for longer than its intended purpose;
- Processed in accordance with the rights of the people the data is about;
- Protected by technical and organisational security measures;
- Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection.

GDPR continues these principles, expands upon them, and adds additional responsibilities.

Who does this affect?

European data protection law is universal and extraterritorial. It applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. It also applies across all sectors, industries, and situations.

This is in contrast to, for example, the United States, which has no overarching data protection regime. Instead, data protection rules there are applicable by sector or state, and often take the form of industry codes of self-regulation rather than enforceable law.

If you do business in Europe, GDPR affects you. This means that GDPR applies to the data you collect and process about Europeans even if your business is not based in Europe and/or has no physical or incorporated presence there.

In the event of a privacy concern or data breach, claims such as "we are not in Europe" or "we were not aware of the rules" will merit no sympathy from Europe's national data protection regulators. Being aware of GDPR, and meeting your legal requirements, is the price of doing business in Europe.

> If you do business in Europe, GDPR affects you.

But what about Brexit?

In whatever form it takes, and whenever it eventually happens, Brexit will mean a withdrawal from the EU data protection regime. It will not, however, mean an immediate withdrawal from GDPR.

The UK government has confirmed that the UK will adopt GDPR and go into it **regardless of Brexit**. This will take the form of GDPR's enactment into UK law as well as supplementary guidelines under the Data Protection Bill announced in August 2017.

GDPR has already replaced the Data Protection Act and it is that, not the 1998 standard, which you should be working to achieve. GDPR will remain the law of the land for some time after the formal divorce from the European Union.

As European data protection law requires equivalency from non-EU third party countries, if you intend to continue doing business in Europe, you must continue to work to the GDPR standard regardless of any post-EU data protection regime that might be put into place in future. In other words, you should prepare for GDPR as if Brexit would never happen and then stay in GDPR as if Brexit never will.

> The UK government has confirmed that the UK will adopt GDPR and go into it regardless of Brexit.

The question of what will happen to UK data protection law several years down the road, both within and outside the Data Protection Bill, is a troubling one. What form will data protection and privacy law take outside an EU standard? Will a UK outside the EU stay aligned to the standards of its European neighbours, or will privacy be watered down to attract American investment? The shape of future data protection law will need vigilance and involvement from digital professionals, and you should be prepared to make your needs clear to government.

As for the immediate future, the proposed Data Protection Bill commits to updating and strengthening existing data protection law. However, the majority of the proposals offered in the statement of intent were things which the UK was receiving in any case under GDPR.

It will be important for digital businesses to monitor the transition to the post-EU data protection regime to ensure that:

1. Data flows and commerce can continue uninterrupted;
2. The post-EU regime offered retains a European standard of privacy protection;
3. The new regime is not in fact the European regime presented under a different name and without credit to its true origin.

What does your business need to do?

Healthy GDPR implementation is an ongoing process incorporated into your everyday processes and workflows. The amount of work that will be required to achieve GDPR compliance within your business depends largely on how much work you had put into compliance with the existing 1995 standard.

Businesses which already had a healthy regard for data protection and privacy will adjust to the new requirements with ease. Businesses which did not will find the new requirements more onerous. For those businesses, the compliance costs and time required for GDPR compliance are the deferred costs of catching up with what should have been happening all along.

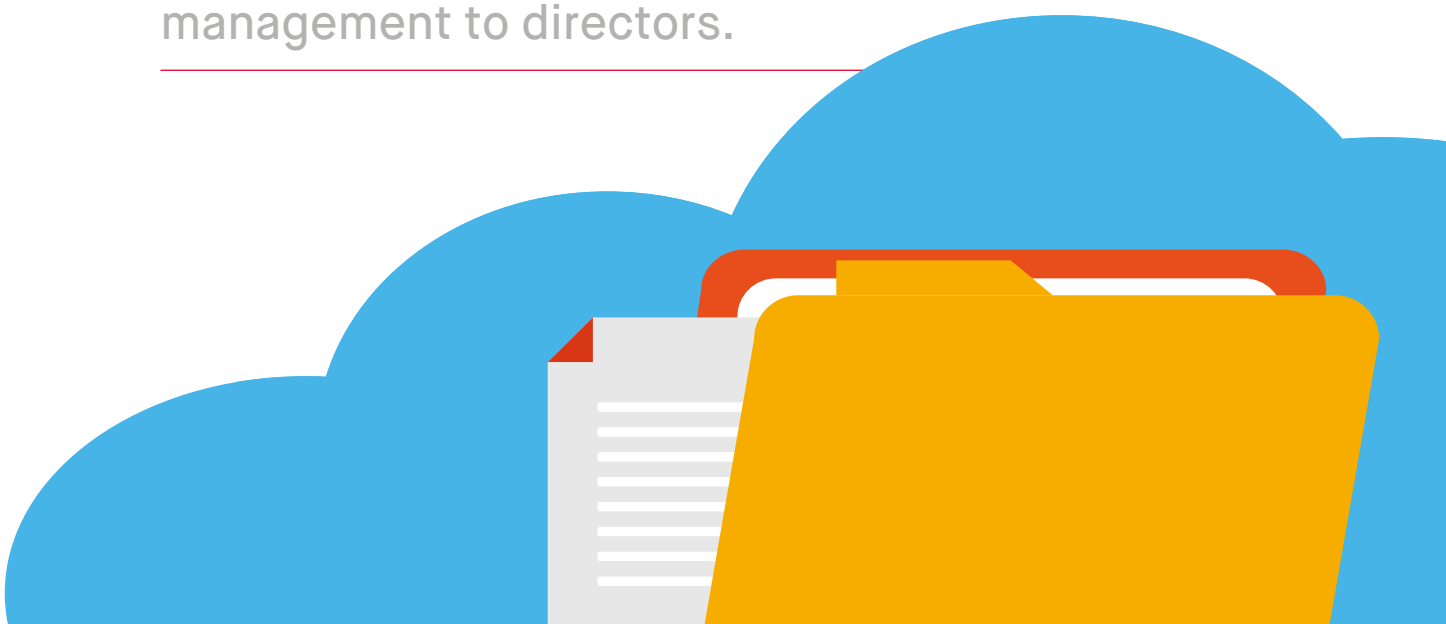
GDPR becomes enforceable on 25th May 2018. Compliance cannot begin on the 25th of April. **You need to start now**. Robust compliance requires clear communication across all levels of your organisation from line staff to management to directors. It crosses departments from IT to marketing to development. There are no shortcuts, tick-boxes, magic software, plugins, or certifications: this is a culture shift, not a compliance task.

There are many ways to approach compliance, and this guide makes no attempt to be an definitive manual on how to do it. But from our perspective, we have found it helpful to split GDPR compliance into three broad areas:

1. Records, information, and communication
2. Protection of individual rights
3. Incorporation of GDPR into our workflows

Let's now explore these steps in depth.

Robust compliance requires clear communication across all levels of your organisation from line staff to management to directors.



Records, information, and communication

Keep records

If we were to sum up GDPR in two words it would be: **document everything**.

GDPR is about knowing what you have, knowing what you are doing with it, knowing where it is stored, knowing who has access to it, and knowing how you are safeguarding it.

You have to know all of this, and you have to document all of this. Some of this documentation will be internal, and some of it, such as your privacy information notices, will be public.

In the event of a privacy concern or a data breach, your national data protection regulator will ask to see your documentation. If that evidence is incomplete, or does not exist, the data breach becomes the lesser of your problems.

Your digital business collects both personal and sensitive personal data as a part of your internal business processes as well as through the provision of your products and services. You'll be aware of this.

There is data you have forgotten as well: old contact form entries retained on databases, email downloaded to local laptops, analytics logs from long-dead projects. What other data have you forgotten, and where is it hiding?

Keeping records is not just about creating inventories. It is about documenting your processes. We'll deal with this in depth later on when we discuss Privacy Impact Assessments.

For now, though, start thinking creatively about what information you hold and how you curate it.

Communication

The most basic step involved in GDPR compliance is making everyone in your organisation aware of the ways the law is changing and how it impacts their work.

This means **everyone**.

It means all staff from the receptionist all the way up to your Board. It means all staff regardless of the nature of their employment, be it salaried, contracted, or temporary staff. It means all staff who handle data regardless of whether data handling is their job.

As we discussed earlier, everything in GDPR must be documented. This includes proof that you have made your staff aware of their obligations. You should incorporate data protection training into your new employee inductions. For existing employees, conduct regular refresher training. Brief your contractors and temporary staff on your data protection procedures. Document all of this on personnel and hiring records.

Your senior management and Board should take a more in-depth look at compliance requirements and should check in regularly to ensure your organisation is on track.

No one expects everyone in your organisation to become experts on the minutiae of data protection. They should, however, be made aware of what personal data is, what you can and cannot do with it, how they should be developing to Privacy by Design, how they should secure consent, what rights people have over their data, what constitutes a data breach, and what internal reporting mechanisms they should trigger in the event that a breach happens.

Privacy information notices

GDPR requires you to be much more public and transparent about the ways you use data. The public face of compliance will be your privacy information notices.

Privacy information notices replace the privacy policies that already exist on your websites and apps. They also replace the days of privacy statements being drafted by lawyers, for lawyers. The language must be simple and plain in a way that anyone can understand. In fact, if your website or app is used by children, you are required to present your policy in language that a child can understand.

Your statement is a dialogue with your users. A dialogue, of course, works two ways. Privacy information notices must give the users of your services real choices and options. Those options should be granular: privacy is not a zero-sum game. The consent they give and the things they consent to, as we will discuss later, can change at any time, for any reason.

Design also comes into play here. Privacy information notices should be presented in an attractive way, preferably a table with icons. In fact, many European data protection regulators are devising standardised templates, and you should check with the regulator in your country to find out what yours should look like.

The UK's data protection regulator, ICO, has set forth the specific information which must be included in your privacy information notices, and you can find that here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

Data protection officers

We have already discussed data protection as being everyone's job. Under GDPR, however, businesses dealing with certain kinds of information need to make data protection an actual job. That job is known as the Data Protection Officer, or DPO.

A DPO does not have to be a lawyer, nor are they required to have any specific set of qualifications. Nor do they need to be in-house: it can be a part-time or contracted role. But the DPO should be competent in the principles of data protection and privacy, committed to the role, and comfortable with raising difficult questions. The DPO must have the authority to challenge anyone across your organisation from the Board on down, and they cannot be reprimanded or even fired for doing so.

Not every business needs a DPO. They are only required for organisations whose core activities involve regular and systematic monitoring of personal data, as well as organisations which engage in large-scale processing of sensitive personal data. They are also required for public authorities. (One way to look at it is this: if you think you might need a DPO, you probably do.)

That being said, businesses outside the requirement are permitted to appoint a DPO voluntarily: a sort of health and safety officer for data protection and privacy issues.

We strongly recommend that every organisation appoints a DPO, either formally or informally, to keep data protection and privacy an everyday concern within your workplace.

Consent

Under GDPR, consent is everything.

In most circumstances, the data collection and processing you may do must be done with the consent of the people that data is about.

Consent must be:

- **Active:** consent is freely given, not enabled by default, and is triggered by the user;
- **Granular:** privacy as multiple choices, not a zero-sum in-or-out. For example, consent to receive a newsletter must not be an automatic opt-in during an account creation process;
- **Unbundled:** users cannot be forced to grant consent for one thing in order to receive another;
- **Named:** the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it;
- **No imbalance in the relationship:** consent must not create an unfair relationship between the user and the data processor. For example, forcing employees to use a company's internal app which monitored employees' location data outside of work hours would be an unfair relationship;
- **Verifiable and documented:** you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

If consent is not given under one of these conditions, then your use of the user's data must be **grounded in a legal basis**. This means that your collection and processing of data must be necessary for the performance of a contract, to comply with a legal obligation, to protect the person's vital interests (such as the emergency services), or for the performance of a task in the public interest or in the exercise of official authority. The legal basis can also be that the data is necessary for the purposes of the "legitimate interests" pursued by the controller or third party.

The exact nature of consent is fiercely debated across industries and data protection authorities, and you should check with your data protection regulator to confirm the current requirements for receiving and verifying consent.

Under GDPR, your users retain legal rights over your uses of their data after they have given you consent - rights which we will now look at in a little more depth.

Protect individual rights

The second broad category for our GDPR compliance process was the protection of individuals' rights over their data.

Europeans have always had rights over the uses of their information under the existing data protection regime. Under GDPR these rights are greatly expanded.

For your business, this means respecting those rights, implementing them into your workflows, and meeting requests to honour individual rights in an open and timely manner.

The user has:

- The right to be informed through privacy notices, which we have already discussed;
- The right to access the data you have collected about them, known as subject access requests;
- The right to correct any errors in the data you hold, known as the right of rectification;
- The right to the erasure of certain kinds of data, commonly known as the "right to be forgotten";
- The right to restrict processing, in other words, your use of their data;
- The right to download their data and take it to another service provider, known as the right to portability;
- The right to object to your processing of their data; and
- Certain rights in relation to automated decision making and profiling, also known as "computer says no".

We will not go into these in too much detail, but we will touch on a few.

In addition to the rights that users can invoke, there are also responsibilities you have regarding data security and breaches.

Subject Access Requests

Under both existing and new European data protection law, an individual has the right to request a copy of the information that you hold about them. This is called a Subject Access Request (SAR).

You can expect to receive SARs from individuals seeking:

- Confirmation that you are processing their data;
- A copy of the personal data that you hold about them;
- A copy of any other information you hold about them, such as details of any data you have passed to third parties, even if the user consented to this.

There are strict time limits for responding to SARs; check with your national data protection regulator. Additionally, because SARs are a basic right, you are not permitted to charge a user any fee or administrative cost for invoking that right.

You must be prepared to respond to SARs quickly, transparently, and cooperatively, and you should devise a SAR process if you do not already have one.

Rectification and erasure

One of the most controversial aspects of data protection law is the right to erasure, which allows individuals to request that a data processor delete their personal data and/or stop processing it.

This is frequently referred to as the much-misunderstood "right to be forgotten" (RTBF).

The RBTF is not a get-out-of-jail card, nor is it means of censoring difficult or embarrassing information. The RTBF can only be invoked if:

- The personal data is no longer necessary;
- The individual withdraws consent for processing;
- The subject objects to processing and there is no legitimate processing need which overrides their request;
- The personal data was unlawfully processed;
- The data must be deleted to comply with a legal obligation;
- The data is about a child.

Even then, the right to erasure is not automatic. A company may continue to hold and processing data about an individual if they still have a legal basis for doing so, and can continue processing that data for its original purpose. (In other words, you can't RTBF your credit card bill.)

In addition to the right of erasure, there is the right of rectification. A user has the right to ask you to correct any erroneous information that you hold on them.

Portability

An interesting provision of GDPR concerns data portability. This is the right to obtain your data and reuse it, if you so wish, on another service.

If you use open source systems such as WordPress you already enjoy the right to data portability. WordPress does not own your content. You can download all your content in an xml file and upload it to any other compatible service you like.

Sadly, not all online services are that enlightened, and so the right to data portability has been brought in to prevent content and user data from being locked behind proprietary walls.

If a person requests a copy of their data, you must be prepared to supply it in a structured, machine-readable, open file format. As with the invocation of all data protection rights, you cannot charge a fee or cost for this right.

If a person's data is mixed with the data of others – for example, someone who has a joint bank account wants to set up their own account at another bank – you must consider and meet the other individuals' data rights in meeting the request.

Profiling, targeting, and marketing

Another aspect of individual rights over data concerns profiling and behavioral tracking. For our purposes, profiling means aggregating multiple data points or sources to generate a picture of an individual's:

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

The GDPR provisions regarding profiling are particularly relevant to advertisers and marketers, as well as to businesses which use their services.

As with all aspects of GDPR compliance, profiling is about to get a lot more granular. Signing up to a service or filling out a form is no longer consent for any number of data-intensive excesses under the name of marketing.

If you are engaging in the profiling of individuals for behavioral tracking or marketing purposes, you must:

- Build in PBDs and PIAs, which we will discuss later;
- Explain clearly and transparently what data is being collected, what it is being aggregated with, and where it is being sent, all of which must be included in your privacy information notices as discussed earlier;
- Obtain explicit and verifiable consent to collect data for profiling, as discussed earlier;
- Responsibly safeguard any sensitive personal data used in profiling;
- Stop processing the data of individuals for profiling when they invoke their rights to do so, under certain circumstances.

Data breach notifications

GDPR requires you to prepare for data breaches in advance. Data breaches, of course, are almost always preventable, so your preparation process is about stopping them as much as possible and then preparing contingency plans for the worst-case scenario.

Under GDPR, certain data breaches must be reported to your national data protection authority within 72 hours. The rule for reporting is that the breach "is likely to result in a risk to the rights and freedoms of individuals."

A high risk breach – one affecting large numbers of people or any sensitive personal data – must be reported to the individuals affected immediately **in addition to** the notification to your data protection authority.

Data breach notifications to regulators must include details about the nature of the breach, such as:

- What category of data has been breached;
- How many individuals are affected;
- How many data records are involved (as opposed to individuals affected);
- Information on how you were alerted to the breach, and by whom (an internal reporting mechanism or a customer complaint, for example);
- Any available information on who was responsible for the breach, or how it happened;
- What consequences will occur as a result of the breach;
- What measures you have taken to deal with the breach, such as contacting affected customers, mass resetting all passwords, and so forth;
- What measures you will take to deal with any results, such as unauthorised charges to customers' accounts;
- The name and contact details of your DPO or the individual taking the lead on the issue.

Although you must report breaches to your regulator within 72 hours, you do not have to reveal any information that would jeopardise your ongoing investigation.

Data security

Under GDPR your data security standards become part of the documented evidence of your compliance.

In the event of a data breach, your data protection regulator will expect to see documentation of things like:

- Password hashing and salting
- Data sandboxing
- Automated updates
- Responsible disclosure
- Penetration testing
- Staff training and accountability
- Physical data security
- Encryption at rest and in transit
- Internal alerts to breaches such as unauthorised data access
- Internal reporting mechanisms

As with all aspects of GDPR compliance, if it isn't documented, it didn't happen. The morning of a data breach is not the time to find that out.

Implement Privacy by Design

The third broad category for our GDPR compliance process has been the incorporation of GDPR into our workflows.

We have discussed GDPR compliance as a function of curating the data you already hold. But what about the new data you will create and collect going forward?

The best way to reduce data protection issues is to reduce the amount of data you have in the first place. Data minimisation takes many forms, but achieving it from the outset can be accomplished by adopting Privacy by Design (PbD) principles into your workflows.

The PbD framework has existed as a voluntary design principle since the 1990s, but GDPR **requires privacy by design and data protection by default**.

You will have to develop in accordance with PbD, and you will have to document your PbD process.

The PbD development principles require that privacy should be:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

In practice this will mean creating specific workflows for data minimisation, establishing defined time limits for data retention, and engaging in regular data deletion.

Moving from a culture of "collect it all, keep it all, and share it all" to "collect the minimum, keep less, and share nothing" will be a major culture shift for many digital businesses. And, perhaps, not before time.

You can find out more about Privacy by Design here:
https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/

Privacy Impact Assessments

Just as the PbD principles have certain required steps, so does the documentation you must assemble to prove your PbD process. This is called a Privacy Impact Assessment (PIA). The PIA should be conducted before you have written a single line of code.

Like all your GDPR documentation, your PIA can be requested by your data protection regulator in the event of a consumer concern or data breach. Do not take the process lightly.

Your PIA workflow can be unique to your organisation or project, and it may be helpful to come up with a template suited to your needs. ICO has some suggestions on how to construct yours.

Regardless of how you construct your PIA, the required steps are:

- Identify the need for a PIA;
- Describe the information flows within a project or service (user to service provider, user to user, service provider to user, user to third parties, service provider to third parties);
- Identify the privacy and data protection risks;
- Identify and evaluate the privacy solutions;
- Sign off and record the PIA outcomes;
- Integrate the outcomes into the project plan;
- Consult with internal and external stakeholders as needed throughout the process.

In addition to using PIAs on your new projects going forward, you should run a retroactive PIA on your existing projects, and take any remedial action required.

Moving data outside the EU

Under EU data protection law, personal data cannot be transferred outside of the EU to third countries unless those countries can guarantee that they work to an equal and adequate level of data protection.

Very few countries do.

If the third country cannot guarantee those standards, companies have a range of legal options for sending data through contracts or intra-company arrangements, such as binding corporate resolutions. These arrangements will require legal advice.

European companies sending data to the US, and the US companies receiving that data, have always been able to use the Privacy Shield framework, a self-certification scheme run by the US Department of Commerce. Companies enrolled in Privacy Shield, signifying a commitment to adhere to EU data protection standards, are listed in a directory on the site.

You should ensure that any US companies you do business with are **Privacy Shield** compliant.

That being said, Privacy Shield has always been fragile and imperfect. Those imperfections have caused it to be the subject of fierce debate and leg al action. That contention had placed Privacy Shield on shaky ground **before** the current US presidential administration expressed sentiments which have **rendered Privacy Shield as good as dead.**

In these volatile times it will be critical for you to monitor the current status of the Privacy Shield framework. Because its survival is not guaranteed, it is all the more important for you, and your non-EU partners, to adhere to EU data protection standards. It may well come to pass that your self-directed compliance is the only thing that allows you to continue doing business.

It is also critical for you to ensure that any third parties you do business with, whether that is a project partner or an ad network, also adhere to EU data protection standards. You should review your contracts and terms of service with them, and make GDPR compliance a required term of business.

You may also wish to review your insurance policies to ensure that you are protected in the event that a non-EU contractor suffers a breach which includes your users' data.

What about noncompliance?

In the run-up to May 2018 you will hear a lot about the penalties and fines that can result from a failure to comply with GDPR. These warnings, sadly, are becoming more exaggerated by the day. (Funnily enough, the most dire warnings are coming from people trying to sell you a GDPR compliance solution. Responsible data protection professionals have even adopted the hashtag "#GDPRubbish" to showcase the worst of it.)

The fact of the matter is that yes, GDPR has teeth. There are two levels of fines for data protection breaches or actionable poor practice. Level 1 fines can be imposed for up to €10,000,000 or 2% of a company's global annual turnover, and level 2 fines can be imposed for up to €20,000,000 or 4% of a company's global annual turnover.

However, those who scaremonger over penalties and fines fail to explain how the system works.

Data protection in Europe is regulated through national data protection authorities. In the UK the regulator is the Information Commissioner's Office (ICO). Regulators can only respond to complaints and concerns raised by consumers. Data protection regulators do have an ongoing proactive engagement with the largest and most data-intensive businesses – such as search engines and social media sites – but for the vast majority of businesses, regulatory involvement is strictly reactive.

Data protection regulators are not parking wardens. They do not have a quota of apps to fine every day. Where a consumer issue is raised, or a data breach is identified, regulators work constructively with the business in a clearly defined, transparent, and non-adversarial process. That process prevents the majority of issues from ever reaching a phase where financial penalties are levied.

When fines are imposed – and they very rarely are – they must be "effective, proportionate and dissuasive" to the matter. Fines only tend to be imposed when the company in question refuses to cooperate, repeats their mistake, or commits a privacy violation so offensive that a fine is the only option possible.

Those who would frighten you into adopting an expensive solution through threats of catastrophic fines do not understand GDPR at all. Data protection is a positive opportunity, a cultural shift, and a mechanism to do right by your users and customers. It is not a weapon, a threat, or a thing to fear. Compliance must start from a position of positive trust, not resentment.

Data protection is a positive opportunity, a cultural shift, and a mechanism to do right by your users and customers.

Short-term actions

We suggest you begin your GDPR compliance process with the following actions:

1. Create an inventory of all the data you hold, both online and offline, internal and external, for active projects and dormant ones.
2. Create privacy information notices for all products and services.
3. Appoint a DPO.
4. Review your consent processes across all projects.
5. Review your Subject Access Request process.
6. Be prepared to meet requests for data rectification and erasure.
7. Implement any data portability processes which might be required for client projects.
8. Review any processes concerning data you use or transfer for the purposes of behavioural tracking or marketing.
9. Review your data breach process.
10. Review your data security standards.
11. Implement PbD into your workflows for all future projects.
12. Create a PIA template specific to your business's needs.
13. Review contracts with any third parties with whom you give or receive data.
14. Review your legal basis for sending or receiving data outside the EU.
15. Share this document with your colleagues.

For more information

UK

In the lead up to 25 May 2018 the Information Commissioner's Office is publishing helpful, plain-English guidance on many aspects of GDPR compliance. Bookmark their page at **https://ico.org.uk/for-organisations/data-protection-reform/** and visit it often.

The ICO also offers free, constructive, non-adversarial advisory visits. ICO staff will visit your office, speak with you and your staff, and identify areas for improvement. You can request a visit at **https://ico.org.uk/for-organisations/resources-and-support/advisory-visits/.**

Europe

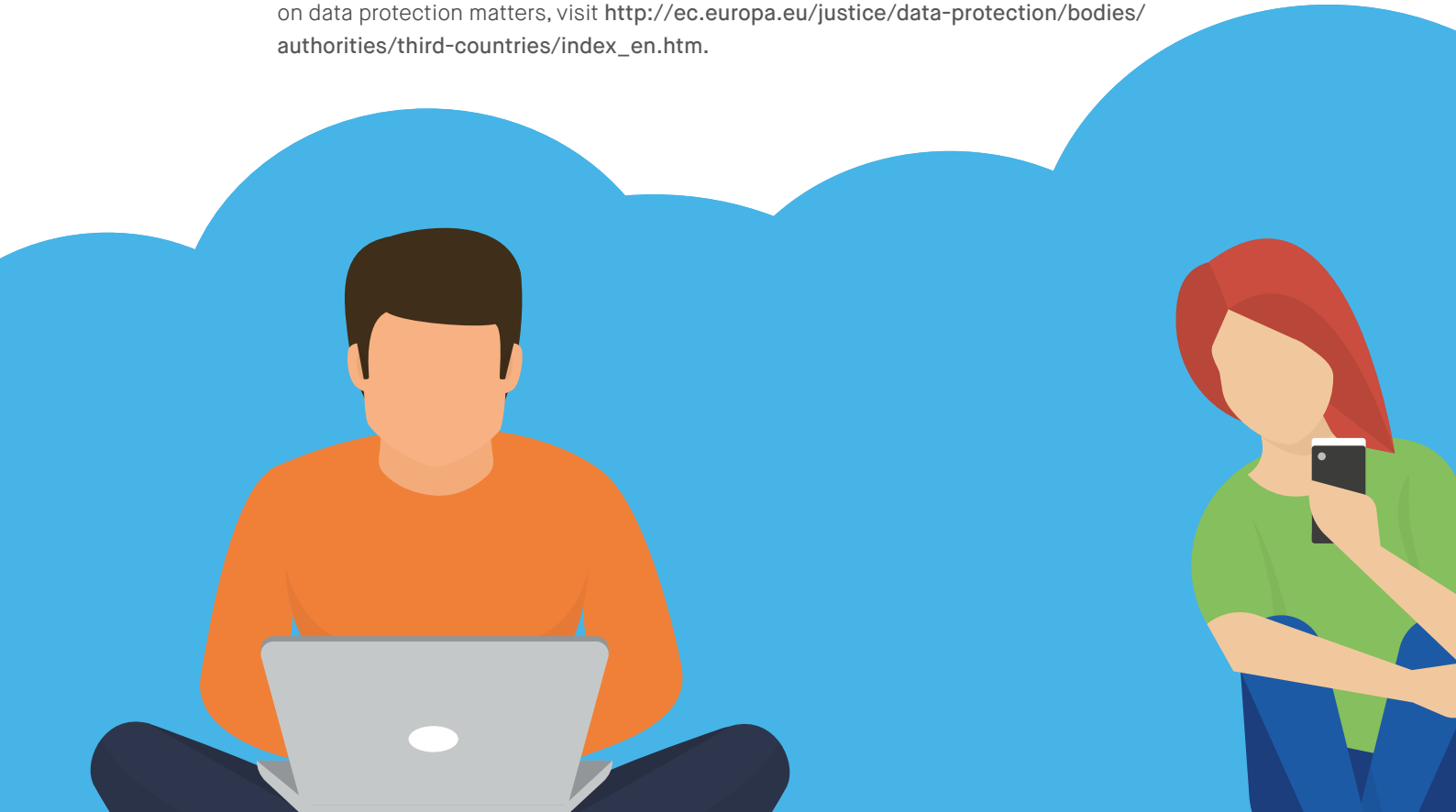
The European Commission has published a plain English introduction to GDPR at **http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm.**

Because European member states are permitted to legislate additional data protection requirements over and above GDPR's baseline, it is important that you check with your national data protection regulator for information on your country's GDPR compliance requirements. A list of regulators is available at **http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.**

Outside the EU

We recommend using ICO's English language guidance for basic compliance information.

For information on specific data protection agreements your countries may have with the European Union and for a list of regulators and agencies which work with the EU on data protection matters, visit **http://ec.europa.eu/justice/data-protection/bodies/authorities/third-countries/index_en.htm.**



If you want to find out more about how GDPR affects your digital estate, get in touch at hello@deeson.co.uk or call us on +44 (0)207 186 8239.

About this guide

This white paper was written by Heather Burns (heather@webdevlaw.uk) who was jointly commissioned by the following agencies (in alphabetical order):

- 93 Digital
- Awesem
- Big Bite Creative
- Connected
- Convivio
- Deeson
- DXW
- Human Made
- MakeDo
- Manifesto
- Pragmatic

Deeson.