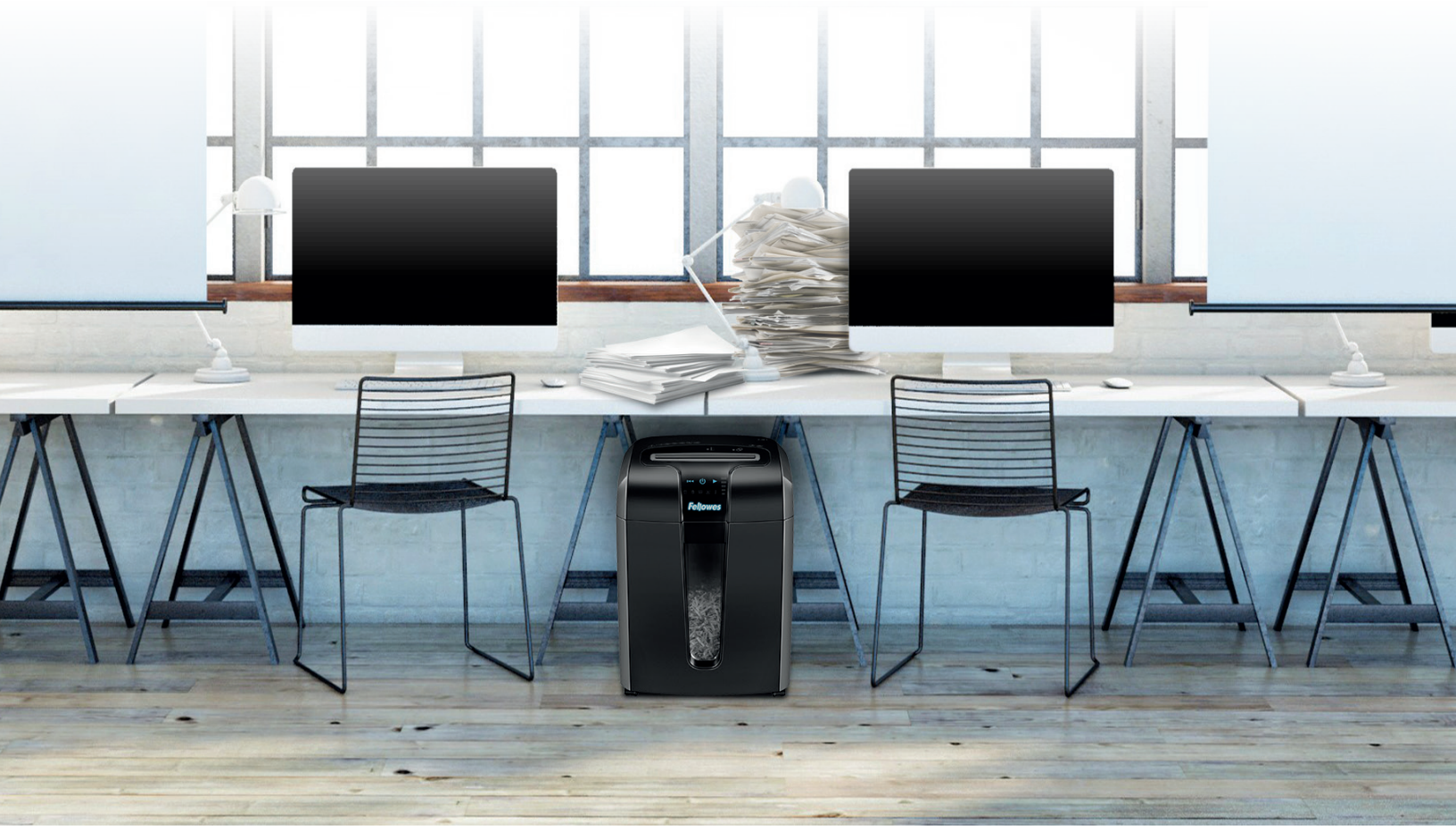
The New General Data Protection Regulation

GDPR

What does it mean for you and your business?



Cordery® Legal.Compliance

Fellowes Brands™

What is the GDPR all about?

The European Union (EU) has changed its data protection rules, which impacts any US company handling EU data. These new rules are called the General Data Protection Regulation (GDPR) and apply across the board from large corporations to small and medium-sized US businesses. The changes are now law.

These changes will affect the way we all do business. This White Paper gives you a basic introduction to the GDPR and especially how it affects companies in the US.

What is EU data protection?

In the EU there are existing legal rules for the collection and processing of personal data. Anyone who collects, or processes personal data must protect it from misuse and comply with a range of legal requirements. These rules apply to US companies as well who work with EU data on any level.

Do these new rules apply to electronic data and hard copies?

Yes. The GDPR will apply to electronic data (like emails and databases) and to hard copies (with a few exceptions). This means that we also have responsibilities with paper-based files – we need to keep them secure and securely dispose of them (for example with a cross cut paper shredder) when we don't need them any more.

You could be fined
$23 million
or 4% of your global annual turnover

What kind of fines can my business face for breaching the rules?

Now data protection regulators can impose a fine of $23 million or 4% of the global annual turnover, whichever is greater.

Will businesses have to do more?

Yes. Every US organization will have more responsibilities and obligations under the new rules. Businesses must implement technical and organizational measures to make sure that they are processing data properly. To assess the right level of security you must consider the risks that are presented by processing – especially from accidental or unlawful destruction. You will also have to be able to show the measures you have taken when a regulator asks you what these measures are. An important part of that is checking who you send personal data to – for example you will also need to check the processes of people you work with like mailing houses, shredding companies and temp agencies.

Will I have to put data protection at the heart of what I do?

Yes. Privacy must be built in to all of your processes. Businesses will have to put in place ways of making sure that, by default, only personal data which needs to be processed is processed.

As a result you'll have to ask yourself:

- Do I need this personal data?
- Do I need to process it for this purpose?
- Does everyone who has access need access (for example if only HR should see the papers should they be locked in a filing cabinet with only HR having keys)?
- Is data out of date?

Will consent be required for data processing?

Yes. Generally-speaking there must be a legitimate reason for processing personal data. If consent is being relied on to process data, under the new rules a person's consent must be freely given, specific, informed and unambiguous. Silence, opt-outs or inactivity can't be relied on and instead an active process such as box- ticking will have to be put in place. Businesses must also be able to demonstrate that consent has actually been given. Make certain that you have processes in place that meet all of these requirements.

Are there any new rights?

Yes. A series of new rights have been introduced including:

- The Right To Be Forgotten – this allows people to ask for their personal data to be deleted;
- The Right To Data Portability – this allows people to ask for their personal data held in a commonly used format to be transferred; and,
- The Right To Object – this includes allowing people to object to being profiled. Where personal data is processed for direct marketing that can also be objected to.

Implementing these new rights will be challenging for organizations, although it should also be emphasized that all these new rights are qualified, i.e. there are some exceptions, for which legal advice should be taken.

What about people asking to see their data?

The right for people to see their data, which is technically called a Subject Access Requests (SAR), continues under the new rules. This process allows anyone to exercise their right to gain access to data held on them. Under the new rules SARs must be answered within one month of receipt of the SAR (although there could be an extension for a maximum of two further months in some circumstances), and, the ability for a business to ask for a fee to respond to a SAR has been abolished. There has been a significant rise in the number of SARs being made in recent years – when SARs become free an even greater rise in SARs can be expected. Given the rise in email and cloud applications in particular, SARs are also now more costly and complex to deal with.

You will need to put proper processes in place to deal with

SARs

*Subject Access Requests

An essential part of any organization's future data protection strategy will therefore be putting proper processes in place to deal with SARs.

Will I need to appoint a data protection officer?

Possibly. Under the GDPR, public authorities must appoint a data protection officer (DPO). The regulation may differ for different private businesses. It is best to take legal advice on this, depending on your industry. Given the significance of privacy compliance today, even when a DPO is not required, medium sized businesses that regularly process data should consider appointing one.

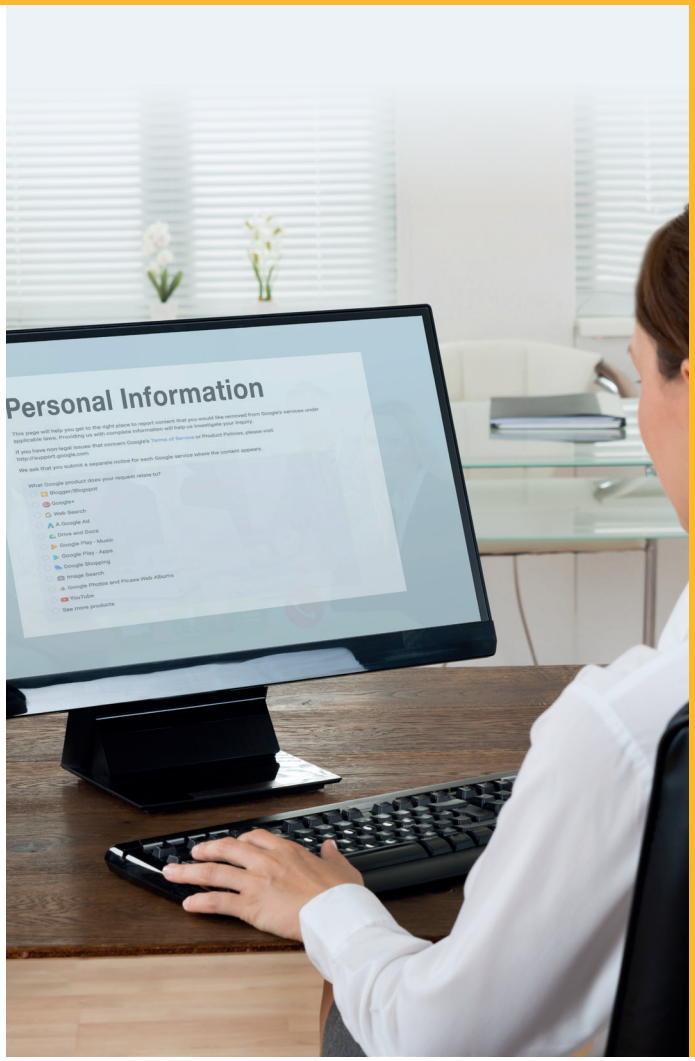
Will I have to report data breaches?

Yes. Ensuring that data is secure is one of the backbones of the new rules including addressing data breaches.

What constitutes a data breach covers many situations including destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Breaches will have to be reported (including what action has been done to mitigate them) to the relevant data protection regulator no later than 72 hours after becoming aware of the breach.

People affected by the breach must be notified within a timely manner, especially when the breach is likely to result in a high risk for their rights and freedoms. There are some limited exceptions for both reporting to a regulator and informing people, for which proper legal advice should be sought.



What about liability and compensation?

As a general principle, anyone who has suffered damage due to an infringement of the new rules has a right to compensation from those controlling or processing the personal data in question for the damage suffered, subject to some exceptions. Because of the extra risk that a data infringement may now bring under the new rules, especially a data breach, businesses will need to do the maximum to minimize the potential for compensation claims.

Businesses must put in place a clear data breach action-plan and policy as a top priority

Will some kind of privacy impact assessments have to be made?

Yes. Under the new rules these assessments are called Data Protection Impact Assessments (DPIAs). Where data processing operations (in particular those using new technologies) are likely to result in a high risk for people's rights and freedoms, an impact assessment of the proposed processing operations on the protection of personal data must be carried out – this must be done prior to the processing.

A data protection regulator must be consulted (also prior to processing) where an assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.

DPIAs are likely to become common and should prove to be a very useful tool for businesses in addressing privacy risks, including assessing data security risk and the consideration of risks presented by personal data processing such as accidental or unlawful destruction.

Has anything changed with data transfers to third countries?

Not really. Special existing rules about the transfer of data from the US to other countries remain in place under the GDPR, including the requirement that those data transfers can only occur where an adequate level of protection is assured by these other countries. Under the new regime these rules have in effect just become more detailed. This is a complicated topic that is also subject to development under the existing data protection rules which you should talk through with your legal team

Where can I find out more?

https://www.fellowes.com/us/en/resources/information-security/gdpr.aspx

What should I do now?

To become GDPR-compliant you must budget and plan resources (including IT). The following are ten top compliance issues to start addressing:

1. Put in place a privacy impact assessment process – map your data and determine areas of risk;
2. Thoroughly review vendor contracts – you will need your vendors' help especially in reporting security breaches very quickly and so make sure that you have the contractual rights to insist on this;
3. Update systems and materials and prepare new detailed documentation and records ready for production for regulatory inspection;
4. Review key practical aspects including data retention with all the data used by the business;
5. Make sure you have plans in place to securely destroy data that you don't need;
6. Ensure that new aspects such as explicit consent, the right to be forgotten, the data portability right, and, the right to object are all included in policies and procedures;
7. Put in place a data breach notification procedure, including detection and response capabilities, and rehearse this like you would a fire drill;
8. Consider appointing a data protection officer;
9. Training, training, training - train staff on all of the above (data protection regulators pay special attention to this).
10. Set up and undertake regular compliance audits in order to identify and rectify issues.


Cordery
Legal.Compliance


Fellowes
Brands