ARE YOU READY FOR GDPR?

April 2018

A HYKER CHECKLIST

Your guide to ensuring that your organization is prepared for the most significant change to data protection regulation in a generation.

HYKER
PROTECTING DIGITAL LIFE

INTRODUCTION

The new General Data Protection Regulation (GDPR) comes into force on 25 May 2018.

Although there are many similarities with the existing data protection laws, there are several additional and more stringent requirements. As a result, the new rules are widely regarded as a 'game-changer' that will transform how we store and process personal data.

Failure to comply with any of the GDPR requirements may result in significant financial loss, disruption or reputational damage to an organization.

But what does GDPR mean for you and your organization?

Are you ready for the most significant change to data protection regulation in a generation?

And how will you ensure that your organization remains compliant with the GDPR requirements on an ongoing basis?

The checklist in this document is designed to help you begin answering these important questions. It will not automatically make you GDPR compliant, but it will provide you with a foundation for your continued analysis.

You may be thinking that this is a lot of work – especially given that there are only a few weeks to go before GDPR comes into force. Just remember that the benefits of proper data management go beyond GDPR compliance. It enables accurate and real-time business intelligence, uncovers customer insights, optimizes marketing and customer service and underpins sounds business strategy and product development.

GDPR overview

The European General Data Protection Regulation (GDPR for short) is built around two key principles.

1. Giving citizens and residents more control of their personal data
2. Simplifying regulations for international businesses with a unifying regulation that stands across the European Union (EU)

It's important to bear in mind that the GDPR will apply to **any** business that processes the personal data of EU citizens which means that it could also apply to companies based outside of the EU.

In the UK the government has confirmed that Brexit will not affect the GDPR start date, or its immediate running. It's also confirmed that post-Brexit, the UK's own law (or a newly-proposed Data Protection Act) will directly mirror the GDPR.

Key Points of the GDPR

Privacy by design: The aim of the GDPR is to protect the Personal Data of EU citizens, including data such as their name, email address, financial or medical details, and even their IP address. A key component of the GDPR is building in privacy from the start in all systems provided by default for all end users.

Data handling: The regulations dictate that organizations should only keep the data they absolutely need for only as long as they need it. Once that data is no longer needed, the data should be destroyed or anonymized.

Right to erasure: Users can request for their personal data to be deleted from an organization for any number of reasons, including suspected non-compliance with the GDPR.

Explicit consent: is **required** for the processing of Personal Data. It must be given freely, and organizations must provide users with the same ease of consent withdrawal should the user wish to do so.

Keeping the data safe: GDPR requires businesses to implement technical and organizational measures to provide appropriate protection to the personal data they hold. Such measures include the pseudonymization and encryption of personal data.

Breach Notification Requirements: In the event of a data breach of Personal Data, the breach must be reported to the Supervisory Authority of the EU member states affected within 72 hours of the breach's discovery. Depending on the severity of the data breach, the organization may also need to notify the affected users as well.

A SIMPLIFIED GDPR TODO FOR THE SMB

Where do you hold your data?

Most businesses will have a CRM system that stores the majority of customer information. However, there will inevitably be a range of other data stores throughout your business. It could be as straightforward as a spreadsheet on your sales manager's laptop or some long forgotten marketing database put together when you were just starting up.

Also, you will have a lot of personal information about your staff in different HR and salary systems. This is also regarded as private information under GDPR. As an employer it is considered part of the employment contract that you should maintain files about your employees, but you are still responsible for the protection of it.

You might be outsourcing many of the internal functions, but it's your responsibility to manage this information and secure how it is transferred to the subcontracted firm. The Hyker Security workspace Konfident.io is a perfect tool designed for this task.

So, to get your data GDPR-ready, you first need to identify all your known stores. Then, list all your customer touch points where data could be exchanged. Finally, ask your staff to check what customer data they hold on their devices or, and this can easily be forgotten, within their email inbox.

Put your data in one place

After identifying all the data you hold, the next step is to get it all into the same format and place. Usually, you will be able to input any new information into your main CRM or sales system. For smaller businesses, a Google Sheet stored in a safe place, like Konfident.io, could be the best approach. Unfortunately, this step can be time consuming and tedious. Just remember the benefits you will accrue and money you will save from doing it properly make it well worthwhile.

Having all information in one place also simplifies a very important task; managing a backup of all your data. Losing a laptop with unencrypted private information is not only a breach of GDPR, it could also be more than an inconvenience from your business point of view if you don't have a backup of the files.

Clean up your data

One of the goals of GDPR is to make organizations more careful about what data is collected. You cannot collect information for its own sake, or information that might be interesting in the future, only the information that is needed.

A similar approach should be taken with the data you currently have. Delete any information you don't need now. The less data you hold, the lower your risk. Delete all copies of the same information that exists outside of your new main store.

Identify your technology gaps

It should now be clear whether the technology you currently have is fit for purpose. If you find that your systems make the above steps impossible or time consuming, it's a red flag that your data management infrastructure needs an overhaul. You should also ask yourself whether what you currently have can scale or is flexible enough to adapt to a new strategy or product offering.

Finally, can you comply with GDPR responsibilities such as immediately porting personal data to customers or completely deleting it under the "right to be forgotten'?

Enforce data governance procedures

The above on getting your data GDPR-ready will be pointless unless you make sure staff understand and follow strict data governance procedures. By using Konfident.io as your document storage you can restrict who can access, collect, store and manipulate customer information which reduces risk considerably. Limiting or banning the copy and storing of data on personal devices or in places other than your main store will also help.

However, the best approach is to fully educate everyone on their responsibilities and the fines that could be levelled. Reviewing these procedures regularly and ensuring they are adhered to will create a company culture that respects personal data and enables long term compliance.

HYKER
PROTECTING DIGITAL LIFE

GDPR Checklist

Preparing for GDPR is likely to be a major challenge for most organizations. The following questions are intended to help you assess how well your data security and usage controls compare to the GDPR requirements and identify areas for improvement.

- □ Have you identified all your data and data sources?
- □ Do you know all the locations where your data resides?
- KONFIDENT.IO □ Have you moved your data to one place? Are the sensitive documents and data stored in a safe place?
- □ Have you classified your data based on a sensitivity and confidentiality level? Do you have data classification policies and procedures in place?
- KONFIDENT.IO □ How is your organization securing its data at rest and in transit? Have you applied data encryption and anonymization techniques where appropriate?
- KONFIDENT.IO □ Can you track who has accessed specific documents containing private information?
- KONFIDENT.IO □ Is all your internal communication containing employee data secure? Do you transfer documents securely to outsourced functions, like HR, salary or accounting? Do you communicate documents, e.g. pay slips, in a secure way to your employees?
- □ How does your organization manage data breaches within 72 hours? Do you have documented procedures to identify, report and investigate a personal data breach?
- □ Has your organization gained explicit consent to hold and use individuals' data? Do you have the ability to check that consent has been obtained for each particular purpose?
- □ Do you have clear guidelines around data retention? Have you defined data retention periods and data disposal policies and procedures?
- □ Does your organization adhere to the 'privacy by design' principle? Is "private" the default for all users?
- □ Are you able to respond appropriately to user requests? Can you provide all the information you hold on an individual promptly and accurately? Do you have processes in place to achieve the 'right to be forgotten'?
- □ Are staff aware of your organization's data protection requirements?
- □ Who is your organization's designated point of contact for data protection? Even though you might not be required to have a Data Protection Officer you still need a designated person with a clear list of responsibilities.
- □ How will your organization ensure it is complying with the GDPR requirements? Do you monitor compliance via internal and external reviews?

KONFIDENT.IO Konfident.io covers this, when your information is in files and documents. Other information must be managed in the appropriate system, e.g. customer information might be managed in a CRM system.