HACKEN GDPR GUIDE

HACKEN

INTRO

Hacken presents its 7 steps to get compliant with GDPR.

The European Union General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive (DPD) and comes into force on May 25th, 2018. A massive change in data privacy regulation is about to take place.

GDPR will set new rules and strict requirements regarding consumer data: the way it is collected, used, transferred, stored, and protected between 3rd party businesses and entities.

Companies that work with European customers in the EU need to make sure their data storage practices are compliant with GDPR and be able to prove it to the authorities.

Security breaches must be reported to supervisory authorities within 72 hours, and businesses must obtain explicit consent from users to collect personal data. Further, users have the "right to be forgotten", and companies are responsible for all costs associated with technology, people, and processes carried by the entity collecting the data.

THE 7 STEPS TO GET COMPLIANT WITH GDPR.

Step 1. Identify personal data and the processes in which they are used

Step 2. Implement the "Privacy by Default" and the "Privacy by Design" principles

Step 3. Minimize the use of personal data

Step 4. Document implementation of the GDPR requirements

Step 5. Obtain customer consent for the processing of personal data

Step 6. Implement information security measures

Step 7. How to react if data breach happens?

HACKEN

STEP 1

IDENTIFY THE PERSONAL DATA AND PROCESSES IN WHICH THEY ARE USED

Personal data is any information related to an identified or identifiable natural person (data subject). First, one needs to come up with an inventory of all per sonal data one holds and examine it under the following headings:

- *Why are you storing it?*
- *How did you obtain it?*
- *Why was it originally gathered?*
- *How long will you keep it for?*
- *Do the principles of encryption, accessibility, and integrity apply to the data?*
- *Do you share it with third parties and on what basis?*

The GDPR's accountability principle requires organizations to demonstrate (and, in most cases, document) their compliance with the main principles of the new legislation when transacting personal data. The data inventory will also enable organizations to amend incorrect data and track third-party disclosures.

Sensitive personal data requires extra protection and consists of data related to the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life. Whether you are aware of it or not, personal data can be found in many places within the systems' storage. Databases are the first place to consider, but personal information can also be found in documents, spreadsheets, emails, and other types of files.

The task of identifying personal data is not an easy one, because it may be found in the ocean of other, non-personal data. Organizations need a tool to automate the process with algorithms that are capable of recognizing personal data and differentiating it from other information.

Once the personal data has been identified and classified, it must be treated and secured in accordance with the GDPR requirements. That's where management, monitoring, and security software and services come in.

STEP 2

IMPLEMENT THE "PRIVACY BY DEFAULT" AND THE "PRIVACY BY DESIGN" PRINCIPLES

The Privacy by Design and the Privacy by Default principles aim to give data subjects more power over personal data. Offering the most privacy-flexible option by default will allow users to choose the personal data they are willing to share. For organizations, implementing these principles is an opportunity to increase efficiency and gain the trust of users.

Privacy by Design requires "data protection through technology design" (Article 25). This means that organizations should ensure privacy at the very early stages of the technology/development and maintain it throughout the complete management process of development of products and services that involve processing personal data.

Privacy by Default means that services should assume the strictest privacy settings by default. If users have a choice regarding how much personal data is shared with others, the strictest privacy settings should apply without any manual input from the end users.

STEP 3

MINIMIZE THE USE OF PERSONAL DATA

According to the general rule, the use of personal data must be reduced to the minimum sufficient level.

The GDPR states that 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" (Recital 39).

The word "necessary" is critical in this context; it means that Data Controllers and Processors can only collect data that is necessary for the purpose of the transaction with the Data Subject. They can also retain this data for a strict minimum period.

Records and data must be eliminated as soon as they are eligible to reduce litigation risks. Data you don't have cannot be compromised!

Minimize user identification wherever it is possible. Embed a function that deletes unnecessary and used data. This step will protect the privacy of users and secure the data in case of a hacker attack. In this case, one won't have to report the breach to authorities and data subjects or pay a penalty for negligent attitude towards the regulations regarding personal data minimization.

STEP 4

DOCUMENT IMPLEMENTATION OF THE GDPR REQUIREMENTS

Companies are required to follow GDPR regulations regarding the creation/maintenance of the necessary documentation to prove they are GDPR-compliant. It needs to be comprehensive and organized in accordance with GDPR standards. Documents should be controlled and use job titles instead of names.

Even with the best policies, tools, and expertise, a company may become a victim of hackers. In this case, it must provide an audit trail of the breach. Not only must the company follow the requirements, but it also has to document the steps it takes to ensure security; undocumented measures will be considered unimplemented.

The audit trial will show that efforts to be compliant to the GDPR were insufficient.

If organizations aren't able to comply with this audit, they face additional fines.

STEP 5

OBTAIN CUSTOMER CONSENT FOR THE PROCESSING OF PERSONAL DATA

The consent must be clear, affirmative, and unambiguous. A person must provide consent by way of a clear and affirmative action, be aware of who is collecting the data, and the purposes of the processing. Further, the information needs to be explained in simple language, introduced separately from the privacy notice and terms of use, specific to the processing activity, freely given (individuals must have a genuinely free choice), and easy to withdraw from.

One must provide comprehensive information on the processing of the user's personal data: what data, when do they go, by whom, where, what for?

The GDPR is clear that controllers must be able to demonstrate that consent has been given. One should, therefore, check the systems responsible for recording consent to ensure having an effective audit trail.

STEP 6

IMPLEMENT INFORMATION SECURITY MEASURES

The regulation has also increased fines for information leakages – companies will not only pay for information leakage with reputation but also face large fines in case they fail to comply.

Companies will be fined for inappropriate privacy attitudes and lack of integrity regarding personal data of users. Product companies will be required to protect their systems since the earliest stages of product development.

GDPR states that organizations must adopt appropriate policies, procedures, and processes to protect the personal data they hold. Article 32 of GDPR specifically requires organizations to do the following:

- Take measures to get data personal data pseudonymized and encrypted;
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- In a timely manner restore the availability and access to personal data should a physical or technical incident happen; and/or
- Implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

There is no single security standard that satisfies GDPR requirements. However, ISO 27xxx certification is one of the approaches that will allow showing the regulatory authorities that you have a solid security management system in place. ISO 27001 is considered the best practice by most professionals - it provides solid evidence of intent and effort to comply. This means that an entity certified according to ISO 27001 Information Security Management System (ISMS) is regarded as one taking a serious approach to protecting personal data in line with the GDPR. Such entities will be treated with greater mercy in case of a data breach.

Ideally, you should appoint a Data Protection Officer to be responsible for checking regulation, implementing and documenting processes, and ensuring compliance with the legislation.

STEP 7

HOW TO REACT IF DATA BREACH HAPPENS?

Companies need to develop proper procedures to detect, report, and investigate data breaches. One of the key reasons that businesses are anxious about the GDPR compliance is the strict data breach notification requirement specified in Articles 33–34: organizations only have 72 hours to report a breach to supervisory authorities.

What is the new Data Breach notification requirement?

Mandatory breach notifications are new to many organizations. All breaches must be reported to the regulatory authorities within 72 hours, unless the data was anonymized or encrypted. Breaches that are likely to bring harm to individuals (identity theft, breach of confidentiality, etc.) must be reported to the data subjects concerned.

A failure to report a breach could result in a fine. This fine is separate from the fine for the breach itself. The consequences for not matching GDPR's requirements are severe. With fees for noncompliance as high as 20 million euros or 4 percent of global annual turnover, companies around the world are taking a second look at how they handle their data.

TO SUM UP

The GDPR replaces the Data Protection Directive and will significantly strengthen people's rights empowering them to demand companies reveal or delete the personal data they hold. Organizations need to review their data protection approaches and be very quick to implement policies, best practices, and technical solutions. Companies who are not prepared for the requirements mentioned above, need to speed in order to avoid reputation loss and possible financial fines.

Recent years have seen a remarkable surge in data breaches. No industry (even having best technologies in place) was lucky to elude data breaches. Remember, technology is just a piece of this puzzle, and companies need to take a comprehensive approach, including developing strategy, educating personnel, analyzing security events and once again, improve security policies and settings.

Thus, cybersecurity has never been more important than today.

Being a cybersecurity company, Hacken has taken care of global data users since its creation. Today, we have a broad range of technical measures for data protection. Including:

- *Anti-phishing services*
- *Pentests of Web, Mobile & IT infrastructure*
- *Cyber Security Assessment and Consulting*
- *BugBounty program as a continuous security approach*
- *Cloud Security*
- *Endpoint protection*
- *Anti-viruses & firewalls, infrastructure security solutions*

Hacken GDPR readiness assessment will not only help to save client's sensitive information but will also sustain own reputation and funds.

HACKEN