Ready for GDPR? Ideas to Update Your Risk Management and Privacy Programs

SECURE HALO

SECURING THE ENTERPRISE

Are You Ready for GDPR?

Protecting personally identifiable information (PII) data at the appropriate new level to comply with GDPR requires an understanding of your data and data flows along with the Privacy Rights of European Union Natural Persons. Complying with GDPR can require some changes in technical controls and processes, which will depend on the current state of your business processes, security controls, and privacy protections.

When it comes to GDPR, many organizations are behind on their security, privacy, and risk management programs. They have not mapped all of their data flows, do not have up to date data inventories, have not defined data retention and deletion requirements, or understand their risks. They have not performed appropriate security assessments, privacy risk or privacy impact assessments to understand what vulnerabilities and risk they possess.

If your organization collects, stores, or processes data of EU/EEA citizens, your organization must comply with GDPR, even if your organization is headquartered outside of EU/EEA countries. Having appropriate evidence of compliance is key. Your organization could be held liable if you are not properly securing personally identifiable information (PII) or sensitive personal information (SPI) as well as honoring the rights of EU/EEA citizens to see what you collect, correct any errors, or even to "be forgotten" by your organization. To avoid potential litigation and penalties, your organization needs to have the programs, policies, and controls in place that will conform your business processes to the GDPR, while retaining your competitive edge.

What is GDPR?

- GDPR stands for General Data Protection Regulation
- Adopted into European Union Law on April 27, 2016
- Enforceable as of May 25, 2018
- Gives individuals control over their personal data
- Applicable to any organization that stores, processes, or transmits PII data of EU citizens
- Non-compliance can result in a fine of up to 4% of annual global revenue or €20 million, whichever is greater
- Penalty for a data breach: up to 2% of annual global revenue or €10 million, whichever is greater
- A personal data breach must be reported within 72 hours of detection to the supervisory authority

Goal of GDPR

GDPR seeks to harmonize the protection of fundamental rights and freedoms of natural persons - that is, individuals living within the EU - in regards to processing activities, and to ensure the free flow of personal data between Member States. The regulation establishes many rights of the natural person.

Some examples are:

- The right of individuals to confirm whether or not their personal data is being processed, where it is processed and why, along with a free copy of data being processed on each and every request of the data subject.
- The right to be forgotten or have personal data erased, dissemination of the data ceased, and processing of the data by third parties halted. This is all under conditions of erasure such as data no longer being relevant to the original purpose for processing, or the data subject withdrawing consent. Requests must be balanced by subject's rights and the public interest in the availability of the data.
- The right to receive personal data in a commonly useable format, and the right to transmit that data to another controller, also known as data portability.

Article 4 of the GDPR defines the roles of **"controller"** and **"processor"** to help clarify the distinction between the two.

(7) **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

EU definition of Personal Data – "Any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Breach Response Time Critical

Under GDPR, unauthorized access to personal data must be reported within 72 hours of data breach detection. In order to meet this tight deadline, it is necessary to have an incident response plan already in place.

Part of developing an incident response plan includes testing it in advance of an incident, as well as to notify and train all involved parties of their respective roles in responding.

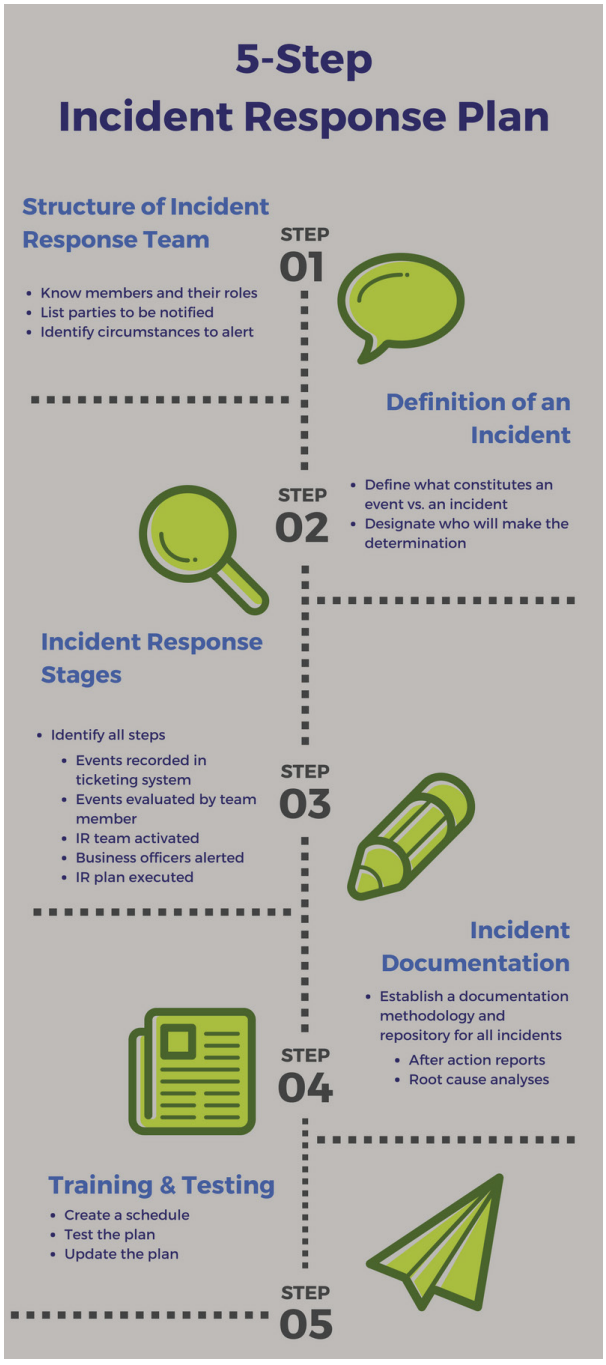
Proper strategic planning and execution will ensure "Privacy by Design," which means under GDPR, organizations will need to consider security and privacy during initial stages of design, as well as during the developmental process. This includes protection controls, safeguards, and incident management throughout the life cycles of processes, applications, and systems.

77%

of respondents claim to not have a formal cyber security incident response plan applied consistently across their organization.

The Third Annual Study on the Cyber Resilient Organization

Conducted by the Ponemon Institute and sponsored by IBM Resilient



The Luxury of Waiting is Over—Act Now

Two years after it was announced, GDPR will go into effect May 25, 2018. It's unclear how quickly and to what extent enforcement will take place, however with the threat of multi-million dollar fines, legal action, and reputation damage from non-compliance, boards of directors and c-suites will place increasing urgency on GDPR preparation. Even after the May 25 deadline, companies will need to demonstrate they have assessed whether they need to be compliant with GDPR and if so, that they have a plan to work toward compliance.

It's important to remember that compliance and security are vastly different. Compliance means meeting regulatory requirements, reducing liability, and preventing fines—it's a bare minimum. Security means taking steps and putting measures in place to protect and secure data and ultimately your enterprise. To achieve compliance and have a robust security posture simultaneously takes an accurate understanding of your specific risk profile, which can be done via an enterprise assessment.

Don't face GDPR challenges alone. Secure Halo has qualified, experienced, and certified experts that can help you. We have both cybersecurity and IAPP Certified Privacy Professionals with concentrations in European GDPR to work with you on identifying and filling your gaps in compliance.

Questions You Need to Ask

1. Has your organization performed a Cyber Risk Assessment or a Data Protection Impact Assessment?
2. Have you reviewed your Privacy Policy?
3. Have you mapped your data flows?
4. Do you know what you have, where it is, and what controls are in place to protect your data?
5. Have you defined methods for capturing Data Subjects' requests?
6. What else do you need to look at?

How Assessments can make your GDPR Planning Easier

Secure Halo will closely work with business data owners to fully understand the following:

Review business processes and specific data inventory

- What types of data (PII) are being collected and what business processes do they feed
- What is the data flow (i.e. what systems are housing, processing, and transmitting that data)
- What portion of that data identifies natural person(s) living in the EU/EEA
- Determine if client is a Controller or Processor or both

Perform GDPR Gap Assessment

- Assessing client's compliance and/or applicability against all GDPR articles
- Perform an assessment of those controls to support GDPR compliance (i.e. monitoring, access control, encryption, psuedonymization, etc.)
- Conduct assessment of information security programs and governance to support GDPR compliance

Deliver comprehensive GDPR assessment report, fully contextualized for the client's business environment

Based on the assessment report, Secure Halo can then perform follow-on GDPR support to include data mapping, data protection impact assessment (DPIA), compliance project management, and program creation and/or modification with documentation.

"If you are a US company and you transmit, collect, or store any data that could identify an EU citizen, your corporation is subject to compliance requirements and, most importantly, the penalties of GDPR. Information security professionals in these corporations MUST take steps to ensure they comply with the requirements to protect this data at the appropriate level with proper controls. In cases of "high risk" to the rights and freedoms of natural persons, a data protection impact assessment should be conducted. Secure Halo has the expertise to guide you through this process."

– Jerry Bujno, Cybersecurity Adviser, Secure Halo

GDPR Readiness: Trust Secure Halo

Secure Halo can help you understand what you do not know. Our holistic approach to cybersecurity, combined with our team's GDPR expertise, will help you identify risks and vulnerabilities, as well as understand your security and data privacy posture. Our DHS SAFETY Act designated assessment methodology involves six primary domains: Internal Business Operations, External Business Operations, Insider Threat, Data Security, Mobility, and Physical Security.

Companies need meaningful insight into how vulnerable they are to expanding and evolving digital risks. Secure Halo delivers enterprise security assessments, managed services, and cybersecurity consulting to Fortune 500 companies and federal agencies. Our Secure Halo™ platform provides a holistic view of cyber risk to empower market-driven and threat-based decisions, while also meeting regulatory requirements.

Learn more at **www.securehalo.com**

SECURE HALO