hardsecure
WE MAKE SECURITY

H-CYBER PRIVACY

(GDPR CONSULTANCY SERVICE)

CYBER EFFECT - LEVEL 1 - REACTIVE

h·cyber PRIVACY

SERVICE DESCRIPTION

Hardsecure provides data security and privacy services in accordance with GDPR. This is the toughest privacy and security law in the world. This regulation it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018, with harsh fines against those who violate its privacy and security standards, with penalties reaching into millions of euros.

VALUE PROPOSITION

If your organization process data, Hardsecure can support it, in accordance with seven protection and accountability principles:

- **Lawfulness, fairness, and transparency:** Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation:** Organization must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization:** Organization must collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy:** Organization must keep personal data accurate and up to date.
- **Storage limitation:** Organization may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality:** Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability:** Data controller with Hardsecure support, is responsible for being able to demonstrate GDPR compliance with all of these principles.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisbon
https://en.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-PRIVACY

(GDPR CONSULTANCY SERVICE)

CYBER EFFECT - LEVEL 1 - REACTIVE

SERVICE FEATURES

Accountability

Hardsecure support data controllers to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how, then you're not GDPR compliant. Among the ways, Hardsecure can support the organization in this:

- Support data protection responsibilities to organization team.
- Maintain detailed documentation of the data that organization is collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- Train organization staff and implement technical and organizational security measures.
- Have Data Processing Agreement contracts in place with third parties that organization contract to process data for you.
- Support Data Protection Officer (internally or Hardsecure will deliver this services).

Data security

Organization is required to handle data securely by implementing "appropriate technical and organizational measures."

Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects to the UE country entity responsible for GDPR audit, or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

H-PRIVACY

(GDPR CONSULTANCY SERVICE)

CYBER EFFECT - LEVEL 1 - REACTIVE

Data protection by design and by default

Hardsecure support everything that organization must do, “by design and by default,” consider data protection. Practically speaking, this means that organization must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in Article 25.

Suppose, for example, you’re launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

Data Protection Officers

Contrary to popular belief, not every data controller or processor needs to appoint a Data Protection Officer (DPO). There are three conditions under which organization are required to appoint a DPO and be supported by Hardsecure:

1. You are a public authority other than a court acting in a judicial capacity.

2. Your core activities require you to monitor people systematically and regularly on a large scale.

3. Your core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR or data relating to criminal convictions and offenses mentioned in Article 10. (e.g. You’re a medical office.)

ADDED VALUE OF OUR SERVICE

There are a host of benefits that the implementation of GDPR made by Hardsecure can bring to your business. Here are just a few:

Enhanced Cybersecurity: Hardsecure services will ensure that only a few people within an organization will have access to critical data, thereby reducing the chance of personal data falling into the wrong hands.

Improved Data Management: Hardsecure will complete a thorough audit to evaluate organization current data management processes to determine if changes need to be made. Hardsecure support the customer to look at the type of personal data held, where it is held, where it was sourced, length of retention, its use, access rights and how it is shared.

H-PRIVACY

(GDPR CONSULTANCY SERVICE)

CYBER EFFECT - LEVEL 1 - REACTIVE

» **Increased Consumer Confidence:** Hardsecure will conduct regular audits of data processing activities and comply with a set of data protection principles that will help safeguard data. This will ensure that a suitable framework is in place that will keep personal identifiable information of customers secure.

» **Improved Return on Investment (ROI):** The GDPR also brings the opportunity for businesses to improve their ROI. The new legislation requires that organisations must have a data subject's full consent in order to process their personal data.

SERVICE QUOTE REQUEST

For further information, please contact us using one of the following means:

"Hardsecure – GDPR Consultancy Service" form (available on the service page on the website)

Contact Hardsecure Account Management:
(+351) 218 278 126 (PT)
(+44) 204 538 6686 (UK)
(+1) 202 2318 9859 (USA)
geral@hardsecure.com

Website:
https://en.hardsecure.com (**"Request Proposal"** form).