

July, 2020

HOW TO PROTECT YOUR CUSTOMER'S DATA

General Data Protection Regulation (“GDPR”) applies to all businesses and organizations established in the EU, regardless of whether the data processing takes place in the EU or not. Even non-EU established companies would be subject to **GDPR**. If your business offers goods and/or services to citizens in the EU, then it is subject to **GDPR**. The protection of employees and client’s data should be the first priority for companies.

Below are some useful information for protecting the client’s personal data:

1. Performing a data privacy audit

The objective of a privacy audit is to assess an organization's privacy protection posture against any legislative/regulatory requirements or international best practices and to review compliance with the companies own privacy-related policies.

2. Minimize data collection and retention (data minimisation)

You must ensure the personal data you are processing is:

- Collected for specified purposes.
- Sufficient to properly fulfil those purposes.
- Periodically reviewed, and you delete anything that is no longer needed.

3. Protect your data

Even if you do not own sensitive information i.e. credit card numbers, other personal data could be valuable to hackers. Therefore, do make sure you are adequately protecting your network, databases, and your website.

4. Publish a privacy policy

Individuals have the right to be informed about the collection and use of their personal data. This is a major transparency requirement under the GDPR. A privacy policy must include the purposes for processing their personal data, your retention periods for that personal data, and with whom it shall be shared with.

5. Provide a platform for complaints

It is very important for your clients to be able to contact you if they have any complaints or questions about their personal data. An online form or e-mail address for them to be able to communicate with any problems or concerns is a very good solution to be provided with. It is very important to respond in a timely manner to their messages. Such communication can build trust and devotion.



Our legal team provides advice to a wide range of organisations (international and local) and undertakes business in both public and private sectors, as well as individuals on all aspects of data privacy, security and information management, including compliance with the GDPR.

Our services include but not limited to:

- Drafting of agreements on Data Processing, Disclosure and Confidentiality.
- Examination of the controls for collecting, processing, storing, retaining and destroying data and providing legal assistance for compliance.
- Issuance of legal opinions on data protection and electronic commerce issues.
- Drafting or reviewing of privacy policies.
- Impact assessments in certain personal data processing activities.
- Legal advice regarding the processing of personal data in the employment context and health organizations and/or companies that are processing sensitive data.
- Content issues, terms and conditions relating to websites.
- Advising on any other data security considerations relating to personal mobile devices and installations of CCTV'S

The purpose of this legal briefing is to provide a general guideline on the subject and not to be considered, in any way, as legal advice. It is advisable to seek professional and legal advice on this subject before proceeding with any general information provided to you. For further clarifications and advice please contact us at legal@economideslegal.com.

Xenia Kasapi, LL.B, LL.M, MCI Arb
Advocate - Head of Data Protection and Privacy Department

xenia.kasapi@economideslegal.com

T: +357 25 866 480