



Don't panic! How to be compliant with the new GDPR in 5 steps

5. Jan 2018

e-Estonia news

The EU General Data Protection Regulation is entering into force on 25 May 2018, with the main goal to harmonize the already existing data protection laws across Europe. The Estonian Parliament is on its way to approve the implementation act to outline new rules for both the public and the private sectors.

In Estonia, the Data Protection Inspectorate (DPI) is the supervisory State agency acting as defender of all information rights, helping to design a society that values the right of individuals to privacy and the transparency of State activities with regards to handling and treatment of data.

We had the chance to interview **Viljar Peep**, Director General of the Data Protection Inspectorate, about ongoing and next developments from a legislative perspective on the matter, both at the Estonian and European levels. A recipe in five points and some interesting insights not to miss your focus on the core issues.

What is the current state of the process of adaptation of Estonian laws so that to be compliant with European General Data Protection Regulation (GDPR) in the transition from directive to regulation?

The implementation act of GDPR is not yet passed in Estonia. Two weeks ago, the Ministry of Justice sent the draft implementation act with the explanatory note to be consulted with the appropriate authorities. The [draft](#) [1] was made public and it is available in the e-Consultation System. The deadline for giving feedback to the ministry is 20th of December. Right now, at the Estonian Data Protection Inspectorate, we are still working on the first draft to give our thorough feedback to the ministry and make suggestions to improve the first draft.

As a follow-up to such kind of assessment, what are the main challenges that companies and the public sector face, in the Estonian context, in order not to incur in falling foul of the rules or sanctions?

First of all, GDPR is not actually about huge fines. Although one might get this impression while reading the headlines and following the news. Questions about GDPR are widely publicized and discussed, but newspapers usually tend to focus on the fines and sanctions. We have to remind ourselves that the new law is actually about greater transparency; it is also about ensuring rights for the privacy of individuals in an age when the economic value of personal data is increasing in the digital economy. The option of imposing huge fines will be the last resort.

The main challenges that companies face in the Estonian context are actually pretty much the same as they are in the other European countries: data portability, carrying out an impact assessment, making sure that all the processes and the documents meet the requirements of the new law.

Portability of personal data: in which ways a data subject can be sure and assured that, at the end of the portability process, previous data controllers won't have access anymore to his/her data?

The portability process does not automatically mean that the first controller has to delete all the data. For example, the client might want to get similar services from two or more service providers; In that case, he can use the right to transmit the data to new provider without asking the first provider to delete it. The data subject has also the right for erasure. In that case, the former controller has to prove he doesn't have the access anymore - unless there is a legal obligation to retain the data (i.e. for taxation purposes).



Right to be forgotten: what are the limits that define public interest of the availability of the data when considering the request of a data subject to exercise the right to Data Erasure?

The right to be forgotten is not absolute, but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media. It is always a case-by-case assessment considering the type of information in question, its sensitivity for the individual's private life and the public interest. It is not always easy to define public interest. Roughly said - when it comes to financial interests of the media, curiosity, gossip, seeking for sensation or entertainment, then it's not about public interest anymore.

Can we outline 5 steps to follow so to be compliant with the new GDPR?

1. First of all - **don't panic!** The foundation of data protection rules is still the same as before.
2. If the processing of personal data is a large-scale process in your company or involves considerable risks, we suggest to **conduct an integrated assessment** of your data processing.
3. **Observe** your entire work order, information systems, and document blanks from the perspective of the new data protection rule.
4. Be sure to **check the data portability** in your work processes and information systems. I forecast that this will be the costliest and most time consuming of the implementing activities.
5. Regardless of whether or not the GDPR requires you to determine a data protection officer, **find a specialist to assist you**. Send your own employee to a trusted training course or make sure an external consultant has undergone relevant training.

[Published in e-Estonia news](#) [2]

Source URL: <https://www.aki.ee/ru/node/1471>

Links:

[1] <https://eelvoud.valitsus.ee/main/mount/docList/1909e111-ca98-4d1b-830a-ee49dea64a97>

[2] <https://e-estonia.com/how-to-be-compliant-gdpr-5-steps/>