Snapshot Corporate

INREV gets ready for GDPR

> Processes adapted to ensure personal data remain secure
> A clear and unambiguous protocol introduced to obtain consent
> Procedures implemented for managing personal data breaches

No one can fail to have seen or heard of the European General Data Protection Regulation (GDPR), which comes into effect from May 25, 2018. INREV like most others will fall under this legislation that will overhaul data protection and privacy rules in the EU.

INREV aims to ensure that 'personal data' is processed in a way that is fair, lawful and transparent to our members. This overview outlines the steps that we have taken.

Tax changes still being actively considered
INREV processes a limited amount of personal data in pursuance of the proportionality and necessity principles as stated in Article 5 of the GDPR (i.e., name of member contact person, his/her company e-mail address and company telephone number). Special categories of personal data as referred to in Article 9, or personal data relating to criminal convictions and offences referred to in Article 10 are not and will not be processed by INREV.

Controller or processor
In terms of 'processor' and 'controller' (Article 4 and Chapter 4), INREV can be seen as the processor on behalf of our members who are the actual controllers of this personal data.

Records of processing activities
We performed an internal analysis based on the criteria in paragraph 5 of Article 3. The results of this analysis were the following:

- INREV is an organisation with less than 250 employees.
- The processing it carries out on behalf of our members is not likely to result in a risk to the rights and freedoms of data subjects (based on a risk assessment using the criteria in WP 248).
- The processing does not include special categories of data referred to in Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.
- However, the processing is carried out more than occasionally.

For that reason, INREV will maintain records of processing activities it carries out for its members in conformance with Article 30.

Security of processing
INREV wants all personal data to remain as secure as possible and has implemented various technical and organisational security measures to safeguard the on-going confidentiality, integrity, availability and resilience of information, (processing) systems and services. For this, the ISO27001 standard is adopted as a guidance.

Examples of information security measures that are relevant for processing personal data within INREV are:

- Information security policies for, among others: information classification, access control, passwords, acceptable use, ethics, mobile device and teleworking, BYOD, disposal and destruction, clear desk and clear screen and usage of social media;
- Policies for assistance of the controller (our members) in compliance with their obligations under Chapter 3 of the GDPR, such as compliance with Article 28 Section 3e, regarding the fulfillment of their obligations to respond to requests for exercising data subject's rights (such as: access, rectification, erasure and/or restriction of processing of personal data), and compliance with Article 28 Section 3f, regarding the obligations pursuant to Articles 32 to 36 in Chapter IV of the GDPR (security and DPIA).
- Procedures for, among others: risk assessment and treatment, incident management, crisis management, data security breach;

- Publication of a Privacy Statement and a Cookie Policy on the website;
- Introducing a clear and unambiguous protocol for obtaining informed consent of data subjects;
- Non-disclosure agreements with suppliers / consultants and confidentiality clauses in employment agreements, including agreements with temporary staff, that are at least equivalent to the requirements set out in INREV's Privacy Statement;
- Attention to information security (including privacy) throughout the design phase of new products and services (privacy by design and default);
- Secure transmission by industry-standard security techniques of personal data from members' computers or devices through the INREV website to our servers;
- Servers are located in secure and controlled environments, protected from unauthorised access, use or modification;
- Only employees who need access to members' personal data to perform a specific task or function are granted access to such personal data. All employees must abide by the privacy statement as stated on our website and the confidentiality clauses in the Employment Agreement;
- Yearly tests on the security of our servers

Personal data breach
INREV has developed and implemented a documented procedure for dealing with personal data breaches that is compliant with GDPR Articles 33 and 34.

Data Protection Impact Assessment (DPIA)
INREV has carried out an internal analysis to determine whether or not a formal Data Protection Impact Assessment (DPIA) according to Article 35 is to be carried out within INREV. The analysis was performed using the ten risk criteria provided in WP 248. This guideline considers that the more criteria are met by the processing operation, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. INREV is not obliged to carry out such a DPIA because the processing of data is not likely to result in a high risk to the rights and freedoms of natural persons.

Data Protection Officer (DPO)
INREV has also carried out an internal analysis to determine whether or not INREV is obliged to designate a Data Protection Officer (DPO). Analysis based on the criteria in Article 37, shows that INREV is not obliged to designate a Data Protection Officer (DPO).

Contractual clauses
Organisations and individuals apply for an INREV membership via an application form in which they agree to the INREV Membership Terms and Conditions that are published on the INREV website. These terms and conditions state that members' data will be treated in accordance with the INREV Privacy Statement.

All INREV contractors either agree with the INREV Terms and Conditions, containing clauses to assure that these contractors treat any personal data they may receive from or process on behalf of INREV, in accordance with the Privacy Statement of INREV, or present INREV with contractual guarantees that are at least equal to the measures and conditions set out in the INREV Privacy Statement.

In the next months, INREV will thoroughly review the application/contract process for becoming a member as well as the GDPR compliance of all our contracts, terms and conditions, disclaimers and privacy statement. Where necessary, improvements will be made that you will be informed about in due course.

A full GDPR compliance statement, revised Privacy Statement and Terms and Conditions will be made available in May. Please note this document is provided as a resource, it is not legal advice.

View all GDPR articles at gdpr-info.eu