PROSPER INTELLIGENCE

APILANi™ Your Enterprise Alliance

EU GDPR – INTELLIGENT RISK MANAGEMENT

The GDPR - INTELLIGENT RISK MANAGEMENT (GDPR - IRM) is commissioned in addition to the GDPR - IRA and is a service which ensures the long - term compliance of our customers.
The GDPR - IRM includes the standardized procedure Audit Upon Procedure (AUP) and is commissioned by our client for a period of 2 to 4 years.

In this procedure, additional functions from our software product ROBOTIC GRC | 365 are used to detect violations of inappropriate handling of personal data in time or to take precautionary action against it. The GDPR - IRM monitors data relevant processes in the entire process, starting from the PC workstation to the contents of their databases and data directories on the servers.

The GDPR - IRM faces the three major challenges of the GDPR, whose permanent implementation means a great deal of time and personnel costs for companies. But since their implementation is mandatory, we have developed functions for this and made them part of our service. In this way we solve for you the three most expensive and complicated requirements of the GDPR:

I. The fulfillment of the Right of access in accordance with Article 15

Following the GDPR - CIA and the GDPR - IRA, we have a map of your IT landscape and a holistic view of your company - wide data processing. Our Cross Database Select feature allows us to aggregate data in a report with criteria of affected persons (for example via a unique identification by a customer number, account number, invoice number, etc ...) across their application landscape. In addition, there is the Cross Workplace Select Feature, which searches all PC workstations according to the same criteria for data subjects and creates a report on identified files. Both features described here are very efficient and can process a large number of requests in parallel and put them together in reports. Compliance with deadlines and the entirety of the report to subjects concerned will be ensured.

II. The right to erasure according to the Article 17

After the data subject requires erasure, we can use our Delete Due Relevance feature to remove data from your systems depending on regulatory compliance without compromising the integrity of your data. A short-term archiving can be activated. This is provided on the system side with an expiry date and will be released after repeated security check by our service for the complete deletion.

III. Notification of personal data breaches according to Article 33

The notification period of 72 hours in case of personal data breach represents a very narrow timeframe. The procedure in this case, has already been established by the company during the preparation. With which information is the notification obligation equipped depends on the case. Especially because it has to be done thoroughly with a description of the nature of the breach and its scope, a description of the expected consequences, a description of the measures taken by the controller and measures for mitigating the damage. Here, the GDPR - CIA with its eDiscovery and the GDPR - IRM prove to be a tool to locate violations in time, to determine the trigger and to estimate the damage immediately. For our customers, this means timely damage control, which in the case of the plunge has a decisive impact on the cooperation with the DPA.

Cooperation with the authorities

The entire service package includes the archiving and recording of all processes in a central data room. This data room is available to the customer at any time. In the case of the control by data protection authority, the central role of the data room is activated. It is available to the authorities as the best possible source of information and signals a high degree of readiness for cooperation.

Checking the audit according to the 'Audit the Auditor' principle

The AUP (Audit Upon Procedure) is a self-initiated audit by the customer by means of a standardized procedure and offers the assurance of performing the best possible survey by an external auditor. The AUP inevitably takes place unannounced, after CIG, regardless of its assessment. This is how it works:

1. All included internal and external positions are visited by our auditor and the accuracy of the annual CIG is checked directly on site. The results of the GDPR - Core Intelligence Assessment are integrated to eliminate gray areas caused by asynchronous operation between IT and business.

2. Part of the audit is the inspection of the business premises in country and abroad. All GDPR relevant documents will be read and a detailed check according to EU GDPR will be made.

3. Detected grievances will be communicated directly to the authorities concerned, followed by a request to eliminate them within the set period of time.

4. The feature of each AUP is the retrospective on previous AUPs, the detected grievances as well as implemented improvements.

Secure maintenance of the documentation

All data and documents that have been collected and checked in the context of the GDPR are stored centrally and enable easy linking with the responsible parties and organizations within the company. The following advantages arise:

1. A transparent overview, which does not allow any gaps and guarantees that the company has achieved a comprehensive compliance.

2. All information can be accessed by the data protection officer at any time.

3. The central storage facilitates subsequent customization activities and improvements and serves the company as a collaboration room with the addition of a good overview of strengths and weaknesses.

4. Our data room provides data protection authorities with a proper handling of the GDPR because it has all the relevant information and signals a high quality standard.

Optimization in handling personal data

Our clients are realistic if they assume that not all positions in their company comply with the GDPR with the same care and quality. Here comes to large deviations independently, whether the processing happens internally or externally. In international companies, cultural differences can lead to great challenges. Here the GDPR- IRM offers:

1. An excellent opportunity to compare the performance of all parties.
2. In the case of vacant differences, a shift in the data processing can be made in order to implement optimizations.
3. We support you with the preparation of requirements for tender documents and with the selection of considered providers.

With our service portfolio we offer the optimal protection for your company.

Call us and we will arrange a conversation

Mobile: +43 664 1033116
Mail: zjo@prosperintelligence.com
www.prosperintelligence.com
Breitenfurterstrasse 378/1/1
1230 Vienna, Austria