iGrafx

WHITE PAPER

General Data Protection Regulation (GDPR): Business Process Management for company-wide Compliance

Oliver Schonschek
Technology Analyst, Insider Research

AT A GLANCE

The implementation of the General Data Protection Regulation (GDPR) is causing difficulties for many companies. Although they only have until May 25, 2018, most companies have not moved beyond isolated solutions to date. This white paper shows how iGrafx's solutions can be used to model, analyze, optimize and automate business processes to achieve complete compliance and implement the General Data Protection Regulation (GDPR) for all processes in a company.

1. General Data Protection Regulation (GDPR) as new compliance requirement

As of May 25, 2018, the new European data protection law, the General Data Protection Regulation[i], abbreviated as GDPR, shall apply. The existing Federal Data Protection Act [Bundesdatenschutzgesetz, BDSG] in Germany shall be replaced; the GDPR shall apply directly in all countries of the European Union (EU). A new German Federal Data Protection Act will establish national data protection rules for the codifying of the GDPR.

GDPR is not only a requirement for companies in the EU, but also for all companies that offer goods and services within the EU, even if they are based outside of the EU (so-called market location principle of the GDPR). Companies are facing far-reaching changes to their data protection processes, which must now be implemented promptly. These include, among others:

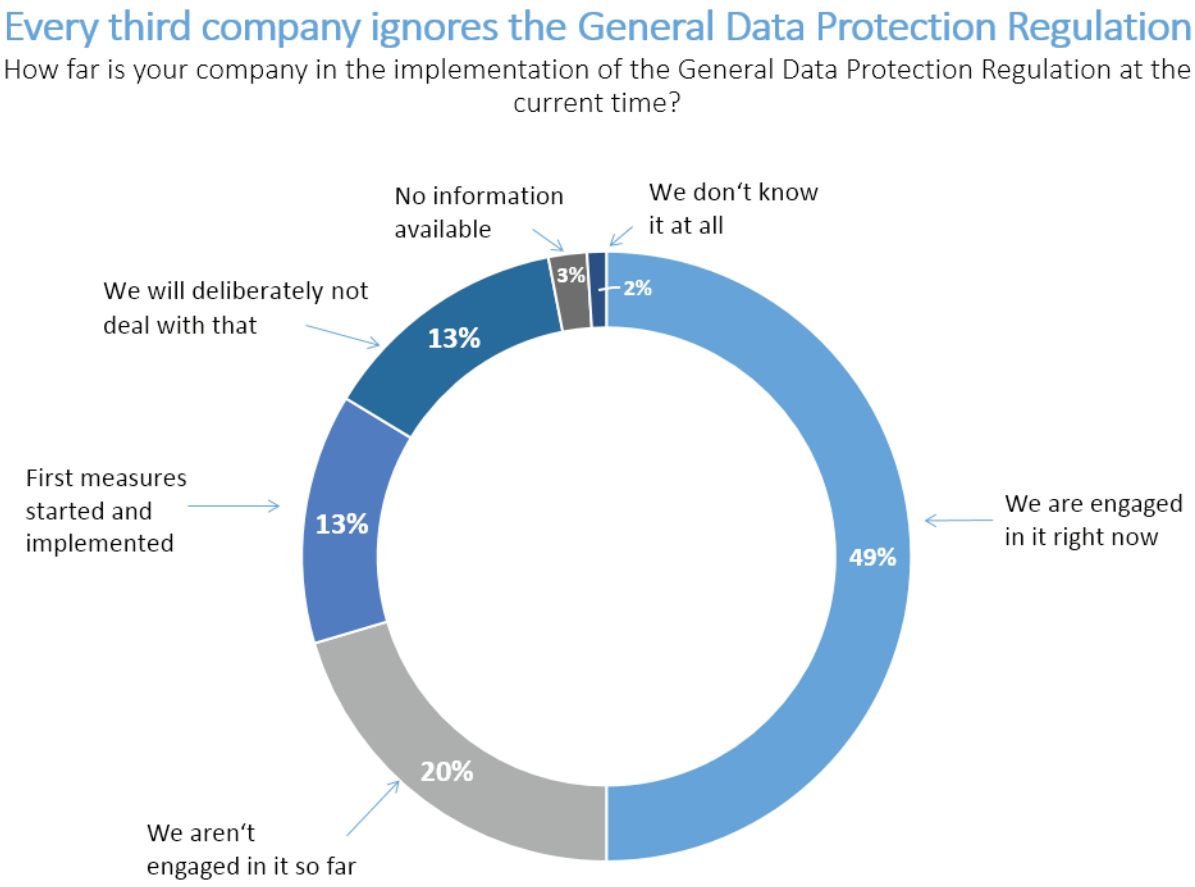
- extended deletion obligations (right to be forgotten),
- new rights for data subjects (right to data transferability),
- stricter reporting obligations in the event of data protection violations (72 hour period),
- new requirements for data processing consent,
- instrument for data protection impact assessment.

Although these new requirements for data protection and thus compliance in a company entered into force in May 2016 and there is a deadline of two years for implementation, most companies have not gone beyond "isolated solutions" – with only individual requirements in the GDPR being picked out – and therefore cannot guarantee complete compliance.

Status of implementation of the GDPR

Various surveys and studies on the implementation of the GDPR show that companies are only concerned – if at all – with individual measures in implementing the GDPR. For example, they focus on the implementation of the reporting obligations or the extended deletion obligations. Accordingly, they only look for and implement isolated solutions that are not suitable for taking account of the entirety of the requirements from the GDPR.

A survey[ii] conducted by the Bitkom Digital Association showed that only 13 percent of companies have begun or completed initial measures for implementing the GDPR. 49 percent are currently addressing this topic. One in three companies (33 percent) report that they have not yet addressed the regulation's requirements at all to date. Of the companies that have already addressed the GDPR, roughly half (47 percent) say that they have completed no more than at best 10 percent of all the necessary work to date. Only 3 percent assume that they have completed more than half of the tasks.



Own illustration based on: Bitkom, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Pressegrafik-Gallery.png

A study[iii] by Ingenium and iGrafx on risk management and business process management shows the following state of risk management and implementation of the GDPR in companies:

- 50 percent of the companies surveyed said that their processes and systems differ in their various departments and areas. Therefore, it is difficult for them to gain a complete picture of the possible risks.
- A quarter of the respondents do not currently have a risk monitoring system in place.
- 62 percent of the companies do not believe that they fully know or understand the effects of the GDPR, and they also do not know what the consequences of the GDPR will be for their risk management.

Additional surveys on the implementation of the GDPR also show:

Companies lack transparency in regard to

- where the personal data is stored, processed and used,
- the purposes for which this is done,
- who gains access to the data,
- who is responsible for the protection of the data and
- how quickly they can react to possible data protection violations or requests from data subjects.

However, it is not possible to guarantee data protection requirements such as deletion obligations, data transferability, reporting obligations, the ensuring of consent or data protection impact assessments without this transparency.

The implementation of the GDPR will not succeed – either by May 25, 2018, or afterwards – without structured processes, risk identification, assessment and monitoring, and without transparency regarding data retention, processing, access, transmission as well as systems and responsibilities. There is, therefore, an urgent need for action.

2. GDPR and Business Process Management

iGrafx Business Process Management solutions make it possible to flexibly design, implement and optimize processes for the entire company. The methods of Business Process Management (BPM) and the iGrafx solutions[iv] are particularly suitable for the obligatory company-wide implementation of the GDPR. The GDPR can be introduced into the business processes as a new compliance requirement by means of the BPM. The GDPR with its specific requirements does not require a special solution, but can be systematically implemented in the BPM with the same methods of modeling, analysis, optimization and automation as all other compliance requirements.

The solutions for implementing the GDPR include, among others, the following:

- All processes and activities in the company that are relevant for data protection can be modeled and analyzed. The data protection measures can be modeled as controls for how personal data is collected, processed and used, as activities such as obtaining consent, and for identifying discrepancies between the actual and target state, which are to be regarded as violations of data protection and which may result in follow-up action such as reports to regulators.

- All data protection responsibilities and access options for personal data can be documented and verified, missing responsibilities and unauthorized access options can be discovered, and resolutions initiated.

- Roles relevant to data protection such as the Data Protection Officer (DPO) or Data Protection Commissioner (DPC) can be defined and assigned to the data protection processes.

- Data protection requirements such as obtaining and documenting consent to data processing can be mapped in the processes and, if required, automated by using the workflow functions (process automation).

- Individual task lists with step-by-step and prioritized task assignments ensure that actions relevant to data protection, such as responding to requests from data subjects, are carried out in a timely and efficient manner.

- Data processing without consent, missing data protection declarations or data transmission without a sufficient data protection level can be detected in the processes as a deviation between the actual state and the compliance requirements.

- It is possible to map and, if necessary, automate rules for when and how process gaps and thus violations of data protection regulations must be communicated and to whom.

- Accordingly, not only can the actual state of the processes be illustrated, but compliance with the GDPR guidelines can also be implemented in a structured way by using process automation. Modeled data protection processes can be automated to ensure ongoing data compliance.

Example: data protection impact assessment

The risk management, identification and assessment in iGrafx's solutions help companies implement and regularly perform a data protection impact assessment as required by Article 35 of the GDPR. For example, users can:

- calculate risks on a user-defined basis in order to take account of how data risk depends on data categories, IT systems used and user-specific parameters, such as the current location of the data processing,

- define risks and controls once and then reuse them regularly to ensure reproducible data protection impact assessments and audits.

If process changes are planned, the solution provides the necessary overview of the consequences and risks: Information on the planned, simulated processes can be compared with available data on existing processes. The solution enables a visual version comparison of diagrams and risk values, making changes visible at a glance. iGrafx provides effective change management and supports data protection impact assessments.

Since a data protection impact assessment should always be carried out in cooperation between the data protection officers and the departments where the new or modified data processing is planned, another feature of the solution helps: It supports effective collaboration and communication by providing all parties involved with the same information in risk management. The solution's central process archive, where processes and related information are stored and managed, is a critical prerequisite for transparency and collaboration in data protection and the data protection impact assessment.

3. Recommendation for implementation of the GDPR

The BPM solutions make it possible to close the gaps in the implementation of the GDPR in a planned, structured way and by having all of those involved in the company collaborate. Companies that have not yet fully implemented the GDPR should now take this step, which can be achieved in its entirety with iGrafx:

1. Recording of the actual situation in the company with the IT systems, data processing (applications), (personal) data and storage locations, processes, roles and responsibilities (process and IT landscape); existing information on the IT and data structures can be imported via interfaces, if possible.

2. Mapping or import of the GDPR requirements as new process and workflow rules.

3. Analysis of the modeled structures and processes, comparison with GDPR rules, identification of gaps in the processes, responsibilities and roles.

4. Assessment of the gaps identified as data protection risk.

5. Initiation of measures to fix gaps, documentation of residual risks.

6. Use of documented processes and controls for the directory of processing activities required by the GDPR.

7. Use of documented responsibilities and workflows for internal training measures.

8. Risk assessment when introducing new processes and procedures by modeling and analyzing the planned state (referred to as the data protection impact assessment in the GDPR).

9. Implementation of regular controls to verify the effectiveness of data protection measures, with the possibility of automating the corresponding workflows and data protection processes.

10. Generation of reports for internal data protection audits and at the request of the data protection regulators.

Conclusion

Instead of just implementing isolated solutions, it is possible to achieve a comprehensive GDPR solution seamlessly that is integrated into a complete solution for company compliance.

More Info?

Are you interested in the concept described in this article?
Visit www.igrafx.com or contact us at +49 8131.3175 0.

Sources:

[i] https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf
[ii] https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Bitkom-Charts-PK-Privacy-Conference-19-09-2017-final.pdf
[iii] http://www.igrafx.com/landing/download.html?name=Risk%20Management%20and%20Business%20Process%20Management%20-%20Survey%20Findings&ao_f=027a&ao_d=d-0001&c_type=c
[iv] http://www.igrafx.com/de/solutions/business-challenges/compliance