

efecte

GDPR

Obligation to provide rapid information



According to the General Data Protection Regulation (GDPR), from the 25th of May all incidents in connection with personal data need to be reported to the responsible regulatory authority within 72 hours. The majority of companies cannot even come close to complying with this timeframe.



**“ By implementing
four fundamental
measures,
organizations
can adapt their
ITSM solutions to
the new information
obligations.**

If an incident entails the loss of personal data, there will be no more hiding: Companies will be required to immediately report corresponding incidents to the responsible [State Data Protection Officer](#) – and that has to happen within 72 hours. The time may appear to be sufficient, but in practice it usually requires a great deal longer.

Just imagine if you will that a former employee downloads all personal data from the company's own CRM application onto a flash-drive and takes this with them. How long do you think it will take until all department managers know which persons are affected by this, who the business owners and responsible data protection officers are and which regulatory authorities for these applications could possibly be relevant? Suddenly questions arise that are unclarified in many companies: An incident and its actual effects must first be analyzed.

With respect to the data protection it needs to be clarified which group of people are effected and which corresponding measures need to be escalated. Responsibilities play a major role in this case: Who is responsible for approving the notification of the regulatory authorities and who is responsible for notifying those effected? The challenges associated with the GDPR suddenly become clear to those responsible for ITSM at the very latest in such a crisis situation. But there is no need to panic, however. By implementing four fundamental measures, organizations can adapt their ITSM solutions to the new information obligations.

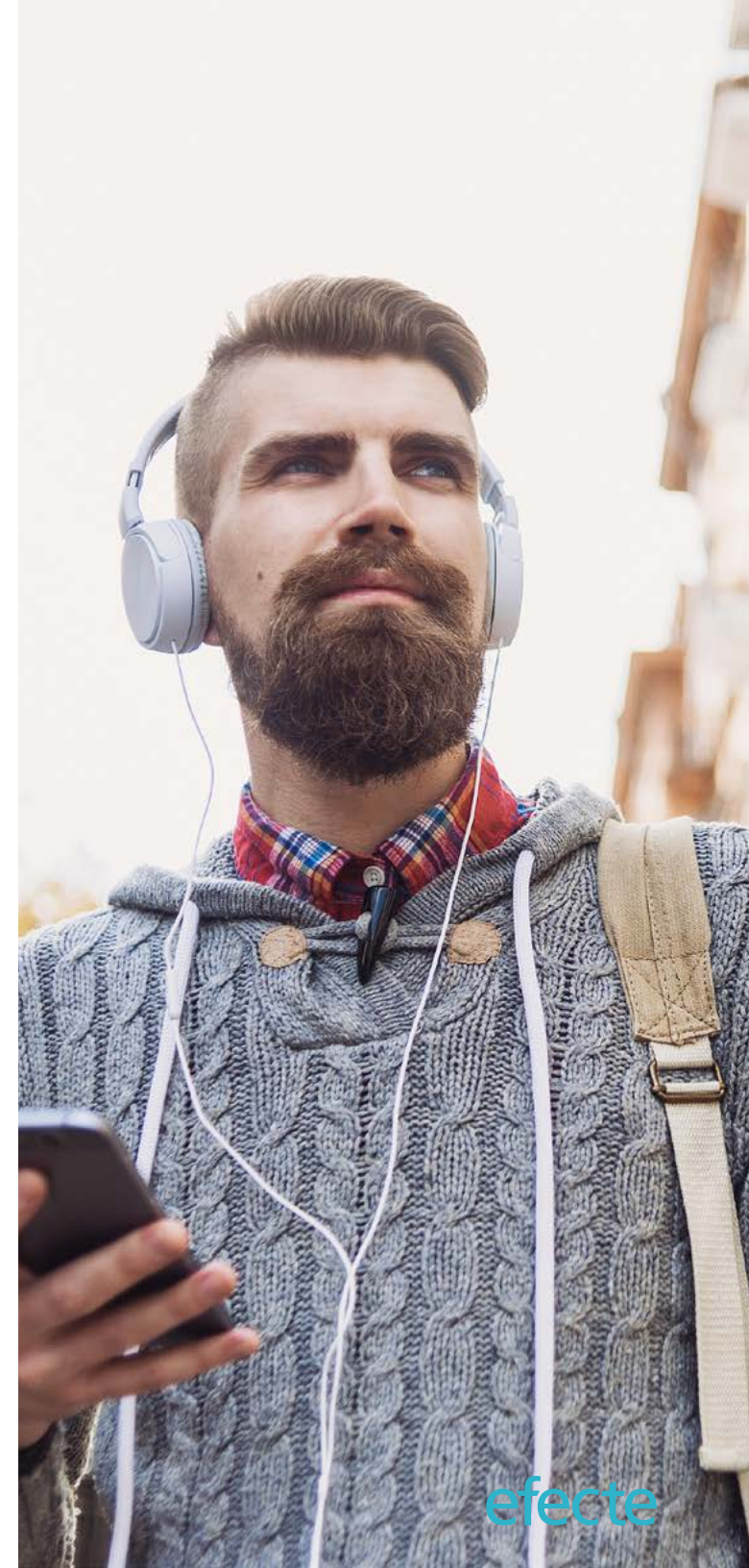
© Copyright Efecte Plc.

All rights reserved. Copyright of this document is vested in Efecte Plc. This document or any part of it may not be translated, reproduced or transmitted by any means for any purpose without permission of Efecte Plc. This document may not be communicated to any third party without permission of Efecte Plc.

1. Structure the GDPR workflow

Typical crisis scenarios are successful hacking and phishing attacks, as well as the theft of credit-card information, personal documentation and other personal information. When the GDPR comes into force, the organizations are required to ensure as comprehensive a flow of information as possible in addition to the actual analysis and damage limitation. In addition to the notification of the Chief Information Security Officer (CISO), Chief Security Officer (CSO) and Chief Information Officer (CIO), the responsible data protection officer and of course the persons effected also must be informed. In order to ensure that this is possible within the required 72-hour time period, those responsible for ITSM must absolutely establish an automatic workflow for all GDPR-related incidents. If a crisis-prevention plan already exists, possible scenarios are usually clearly defined and can be transferred into a workflow relatively quickly with the help of common ITSM tools.

Whereas if this is not possible, then an acute necessity for action to be taken exists: CIOs, together with the managers of the IT and technical departments, should identify the problem fields and scenarios with respect to saving, transfer and processing, as well as all the required steps that need to be implemented in the event of a crisis. If this has happened, the service management could also take corresponding precautions. In short: A standardized approach helps organizations to take a formal approach to managing problems or crisis situations around everything to do with personal data. This provides those responsible with an overview and allows them to concentrate on the actual problems. This also allows them to avoid unnecessary costs that could arise as a consequence of an infringement of the information obligation at the same time – and this also includes the on-time notification of the responsible state data protection officers. In order to effectively utilize the workflow, further measures are necessary, however.





2. Compile a central list of relevant contact partners and regulatory authorities

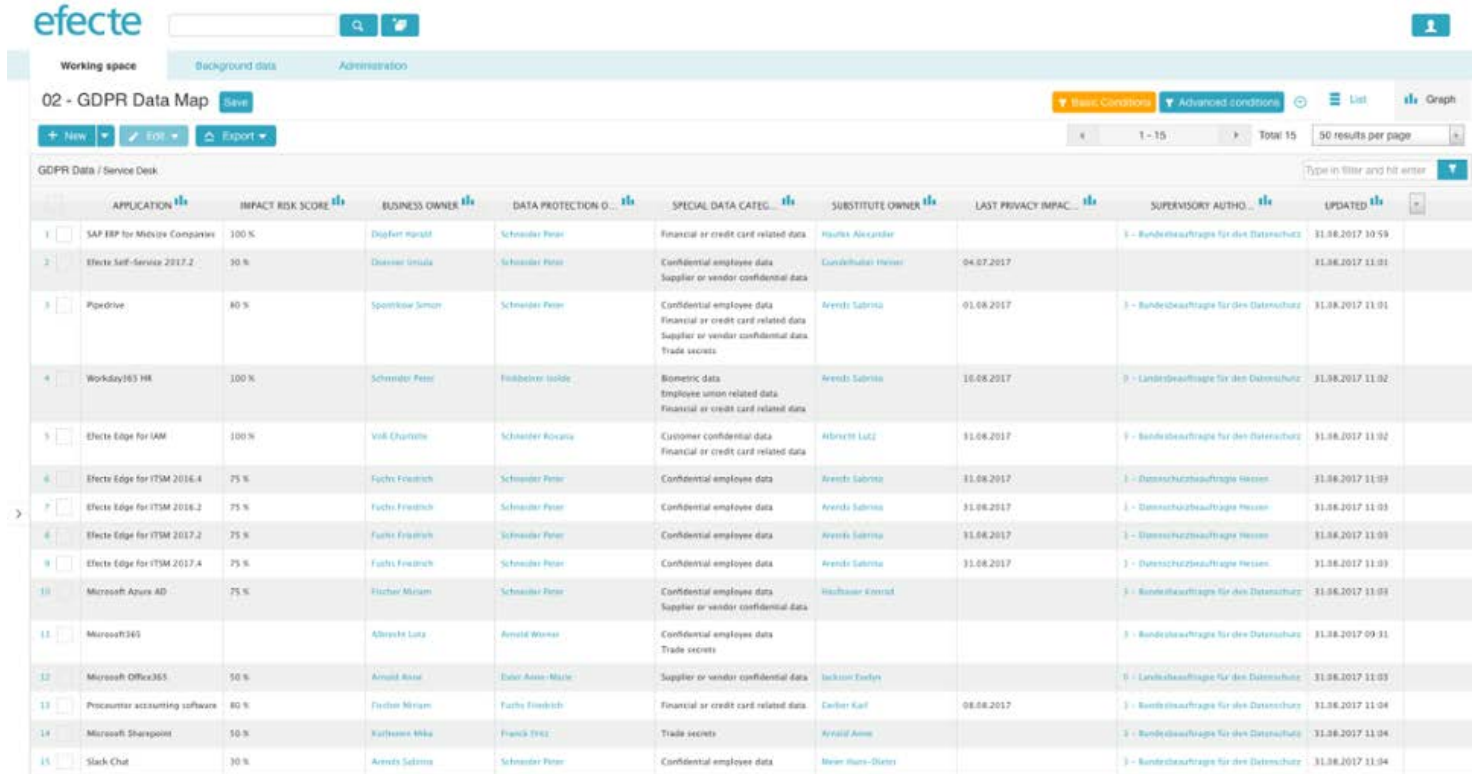
Timely received information is important, but without the correct addressees, valuable time is also lost during a crisis incident. This can be avoided however. The contact information for all regulatory authorities within the European Union are freely available to the public. The same applies for the data protection officers of customers and business partners. Then why not save all relevant contact information with a centralized body? Modern ITSM solutions can be expanded with corresponding data fields at a relatively low costs. If the missing information is sensibly integrated into the GDPR workflow, this compulsory information process can be decisively accelerated.

3. Formulate legally secure notification texts

In the event of data being stolen, companies data protection officers are required themselves to notify the state authorities and, of course, those effected. In crisis situations, for all involved it is all about having the most clear, legally-secure and, in particular, individual information. Organizations should ensure that those responsible are provided with approved templates for varying information texts and that these can be saved in existing ITSM and ESM solutions. The preparation that need to be made for this require the close coordination between the technical and legal departments, as well as the communication team. But the effort is worthwhile, however, because in the event that a data protection problem should arise, the information process can be accelerated massively and can even be automated in many cases. Advantages: IT and security experts can analyze the situation and immediately implement countermeasures or quickly install backups.

4. Creation and maintenance of a data card

If a crisis situation arises and companies are not prepared to deal with them, those responsible for ITSM and the management must tediously ascertain which application is effected, where personal data is involved and exactly how critical the situation in fact is. This challenge can be solved with a detailed data card. It contains information on business applications applied across the entire company. It usually shows in table form where which personal data is saved and which applications and employees have access to this information. It is also possible to save here whether regulatory authorities actually need to be involved at all and who possibly needs to be informed.



The screenshot shows the 'efecte' GDPR Data Map interface. The table lists various applications and their associated data processing details. The columns are: APPLICATION, IMPACT RISK SCORE, BUSINESS OWNER, DATA PROTECTION O., SPECIAL DATA CATEG., SUBSTITUTE OWNER, LAST PRIVACY IMPAC., SUPERVISORY AUTH., and UPDATED.

	APPLICATION	IMPACT RISK SCORE	BUSINESS OWNER	DATA PROTECTION O.	SPECIAL DATA CATEG.	SUBSTITUTE OWNER	LAST PRIVACY IMPAC.	SUPERVISORY AUTH.	UPDATED
1	SAP ERP for Mexico Companies	100 %	Diapfen moralt	Schneider Peter	Financial or credit card related data	Houtke Alexander		5 - Bundesbeauftragte für den Datenschutz	31.08.2017 10:59
2	Efecte Self-Service 2017.2	90 %	Oliverio imala	Schneider Peter	Confidential employee data Supplier or vendor confidential data	Gundelhuber Heiner	04.07.2017		31.08.2017 11:01
3	Pipedrive	80 %	Spontkrow Simon	Schneider Peter	Confidential employee data Financial or credit card related data Supplier or vendor confidential data Trade secrets	Arendt Sabrina	01.08.2017	3 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:01
4	Workday163 HR	100 %	Schneider Peter	Freiburger Isabelle	Biometric data Employee union related data Financial or credit card related data	Arendt Sabrina	16.08.2017	9 - Landesbeauftragte für den Datenschutz	31.08.2017 11:02
5	Efecte Edge for IAM	100 %	Voll Christoph	Schneider Roxana	Customer confidential data Financial or credit card related data	Albrecht Lu2	31.08.2017	5 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:02
6	Efecte Edge for ITSM 2016.4	75 %	Fuchs Friedrich	Schneider Peter	Confidential employee data	Arendt Sabrina	31.08.2017	3 - Datenschutzbeauftragte Hessen	31.08.2017 11:03
7	Efecte Edge for ITSM 2016.2	75 %	Fuchs Friedrich	Schneider Peter	Confidential employee data	Arendt Sabrina	31.08.2017	3 - Datenschutzbeauftragte Hessen	31.08.2017 11:03
8	Efecte Edge for ITSM 2017.2	75 %	Fuchs Friedrich	Schneider Peter	Confidential employee data	Arendt Sabrina	31.08.2017	3 - Datenschutzbeauftragte Hessen	31.08.2017 11:03
9	Efecte Edge for ITSM 2017.4	75 %	Fuchs Friedrich	Schneider Peter	Confidential employee data	Arendt Sabrina	31.08.2017	3 - Datenschutzbeauftragte Hessen	31.08.2017 11:03
10	Microsoft Azure AD	75 %	Höcher Miriam	Schneider Peter	Confidential employee data Supplier or vendor confidential data	Hochbauer Konrad		3 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:03
11	Microsoft365		Albrecht Luca	Arnold Werner	Confidential employee data Trade secrets			5 - Bundesbeauftragte für den Datenschutz	31.08.2017 09:31
12	Microsoft Office365	50 %	Arnold Axel	Daler Anna-Maria	Supplier or vendor confidential data	Jackson Evelyn		6 - Landesbeauftragte für den Datenschutz	31.08.2017 11:03
13	Procounter accounting software	80 %	Fischer Miriam	Fuchs Friedrich	Financial or credit card related data	Dalber Karl	08.08.2017	3 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:04
14	Microsoft Sharepoint	50 %	Karlsson Mike	Frank TH2	Trade secrets	Arnold Anne		3 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:04
15	Slack Chat	90 %	Arendt Sabrina	Schneider Peter	Confidential employee data	Neen Hans-Dietrich		5 - Bundesbeauftragte für den Datenschutz	31.08.2017 11:04

Conclusion: IT manager and service manager become change agents

The basic data protection should install new regulations on how to handle personal data. Practice will show if this can actually be successful across Europe. But this is certain: Organizations need to be prepared for this – whether they want to be or not. Similar to Enterprise Service Management (ESM), corresponding projects are often started in IT and are then extended on a step-by-step basis to other departments. The IT department is functionally responsible. IT managers should be conscious of this situation and quickly begin with the preparations. The IT manager and the service manager have a particular role to play in this: they can prepare their teams on the basis of the existing ITMS solutions best practices and then take an active part in moving corresponding projects forward. Thus, they become change agents for the entire company. One thing that should also be kept in mind here is: just like each IT project, the implementation of the GDPR is a team achievement. Corresponding projects can only then be successful when all users are convinced and work together in a productive manner. It therefore makes sense to bring the CIO on board early and to quickly get the managers of each technical department involved.