perspectium

General Data Protection Regulation (GDPR) and the Implications for IT Service Management

February 2019

WHITE PAPER

GDPR: What is it?

"The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy, and to reshape the way organizations across the region approach data privacy."
Source: EU GDPR Portal, https://www.eugdpr.org/

Under GDPR, as of February 2019, over 59,000 breaches of personal data were reported, and 91 fines were imposed.
Source: DLA Piper GDPR Data Breach Survey: February 2019, https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/

GDPR was adopted by the European Union (EU) government in April 2016 and became enforceable on May 25, 2018. The intent of the new regulation is to protect EU citizens from the privacy and data breaches that are far more common than when the previous data privacy rules were written in 1995. The old rules were open to interpretation by each country, and did not lay out real implications or penalties for failing to comply. As a result, not enough was done to protect personally identifiable information (PII) data as technology evolved, and the world became more data-driven.

The two most significant differences of GDPR from previous standards are:

1. The regulation applies to data for any EU citizen, no matter where they reside in the world and no matter where data processing takes place in the world.

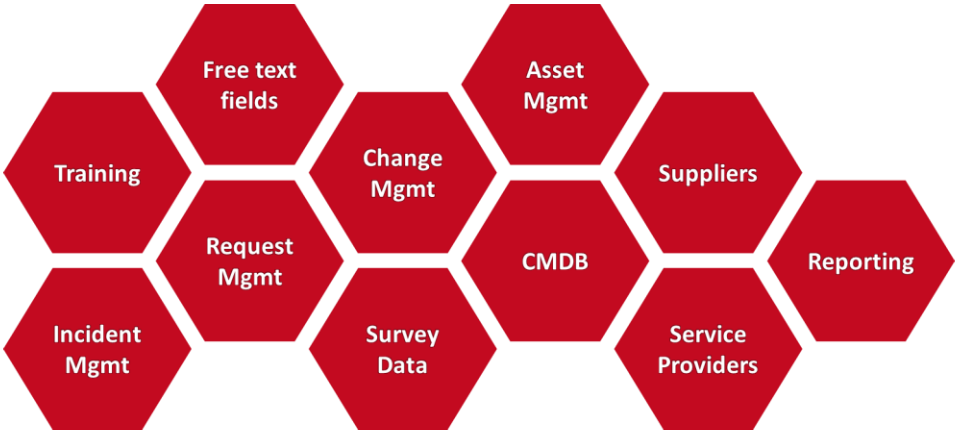
2. There are clearly defined penalties for failing to comply: up to 4% of annual global turnover or €20 Million, ***whichever is greater***.

Make no mistake: although enacted by the EU, this is a truly global regulation that impacts a high percentage of companies and government organizations in the world. If you employ EU citizens, if EU citizens reside in your jurisdiction, or you process data relating to EU citizens, then GDPR applies to you. Also, recognize that world-class data security does not automatically equate to world-class privacy: they are two separate functions, each needing policy, process, and technology to ensure compliance.

The GDPR spotlight has shone mostly on the implications for Human Resources, who manage PII data for employees, and Marketing who capture, purchase, and use PII data to make contact with customers and prospects. But the reality is that the impact on IT is considerable, given its responsibility for storing, managing and moving data on behalf of the organization. In this white paper, we'll outline some of the major requirements and discuss ways in which IT can support a smooth adoption of GDPR-approved practices.

What Does GDPR Mean for IT Service Management?

There are seven different areas of regulation within GDPR, including consent, right to be forgotten, breach notification, and data portability. Across all of them, the challenge for IT is how to manage PII data about employees, customers, and partners. In particular, the issue of how to assure privacy and security of data as it moves between systems – especially where 3rd party service providers are involved – needs special attention in order to comply with GDPR outlines. As with any major IT project, IT service management is central to the process of requesting service, responding to issues, managing the assets on which PII data resides, and collaborating with other key groups to ensure GDPR compliance can be achieved and maintained effectively.



IT service management functions impacted by GDPR

Training: You need to provide specific awareness, education and training for all data handlers.
Free format text: If you use free format text fields, you are now required to provide extra training and support for their service desks so they can properly examine the input of data and scrub any personal or sensitive data. This could be a laborious manual process.
Request, Incident, Change: ITSM users need to have a transparent policy for request management, a policy on the collection of PII data that is held in incident and change management. Explicit consent is also required from users who are likely to raise incidents or authorize or implement changes, with very careful consideration going into the process of what can be entered into the free text fields.
Surveys: Service desk performance surveys require explicit consent from the users who are chosen to be surveyed.

Asset and Configuration: There is significant impact on the ownership of IT assets in configuration and asset management, as asset owner's name, job title and email address are all present in both of these modules. This includes data about what devices are deployed, where they are, who has access to them and what data they access.
Suppliers: IT suppliers are now jointly liable for any data breach, meaning that all policies, processes, procedures and contracts with businesses relating to the handling of personal data need to be reviewed and potentially overhauled. This has implications across, not just service and system providers, but also the suppliers of cloud computing and storage.
Service Providers: Organizations are no longer able to rely on third parties to safely store or process their data sets on the basis of ordinary assurances. IT departments will therefore need to ensure that cloud vendors are compliant with the GDPR when storing, securing, and processing data.
Reporting: Organizations need to identify all locations of a user's personal information – to provide to the user, or to delete at their request.

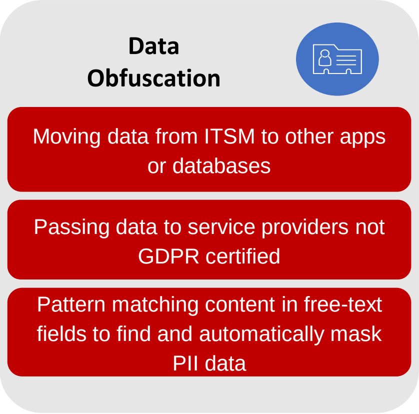
Perspectium Integration Solutions

Rightfully, considerable focus is given to business processes and policies, and to the applications in which data is managed, when it comes to GDPR compliance. But privacy of data while it is being moved is also a key factor, and that is where a strong integration solution can help IT meet and maintain compliance requirements.

Perspectium's integration solutions for IT service management provide data services that offer three primary ways in which to protect data privacy, both within ITSM systems and when in transit to other systems.

1. Data Obfuscation

Data obfuscation is the process of hiding original data with random characters or other data. This renders the original data unintelligible to users or other systems which do not have the authority to view it. For GDPR, this could include names, phone number or email addresses, social security numbers, or other PII data captured as part of the service delivery process.



Data Obfuscation

Moving data from ITSM to other apps or databases

Passing data to service providers not GDPR certified

Pattern matching content in free-text fields to find and automatically mask PII data

2. Process Enforcement

Perspectium service integration operates at the process level, allowing for workflow rules and criteria to directly impact how, when, where, and for whom service integration can happen.

Integration at the process level is key here, to allow workflow criteria rather than a certain time of day to be the trigger for integration actions.

Process Enforcement

Auto-escalate breach notifications to ensure GDPR notification happens within 72 hours

Enforce workflow on surveys to ensure only users who have given consent are surveyed

Automate GDPR compliance checks as part of employee off-boarding, to allow the option of PII data removal if appropriate

3. Deletion Requests

“Right to be forgotten” is a key requirement within GDPR. If a user requests the removal of their personal data, or if workflow identifies data that is deemed inappropriate and a removal request is auto-created, IT must comply. This may involve collating PII data from multiple systems for validation by the user, so integration has to be able to bring together and standardize the required data. It’s also possible that data is being held on systems at external suppliers or service providers, and that data must be included in deletion requests.

Ideally workflow should automate and enforce the request/approval process so there is an audit trail to prove completion of the deletion of the user’s data.

Deletion Requests

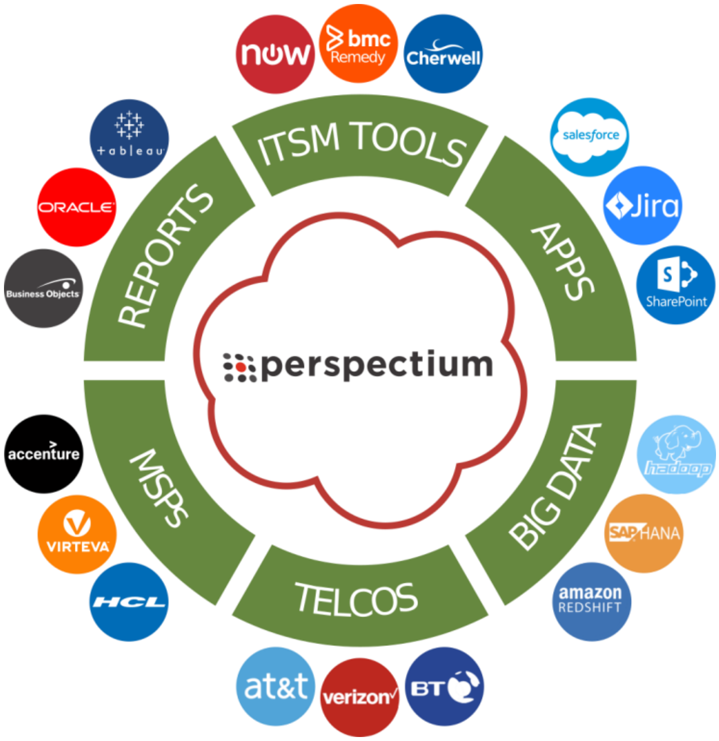
Auto-create privacy removal requests when PII data is identified in the system

Identify and consolidate PII data from multiple systems, to provide to the user, or to identify for deletion at their request

Ensure collation and removal of PII data from external supplier systems

Complying with GDPR

Companies are documenting processes, implementing privacy standards, and applying technology to automate and accelerate compliance relating to GDPR. IT service management can be a complex function, central to many activities where the management of PII data is a normal part of daily life, and it is exactly this complexity that Perspectium integration solutions can help ease.



If you would like to learn more about how Perspectium integration solutions can help you reduce complexity and eliminate some of the barriers to achieving GDPR compliance, visit www.perspectium.com.