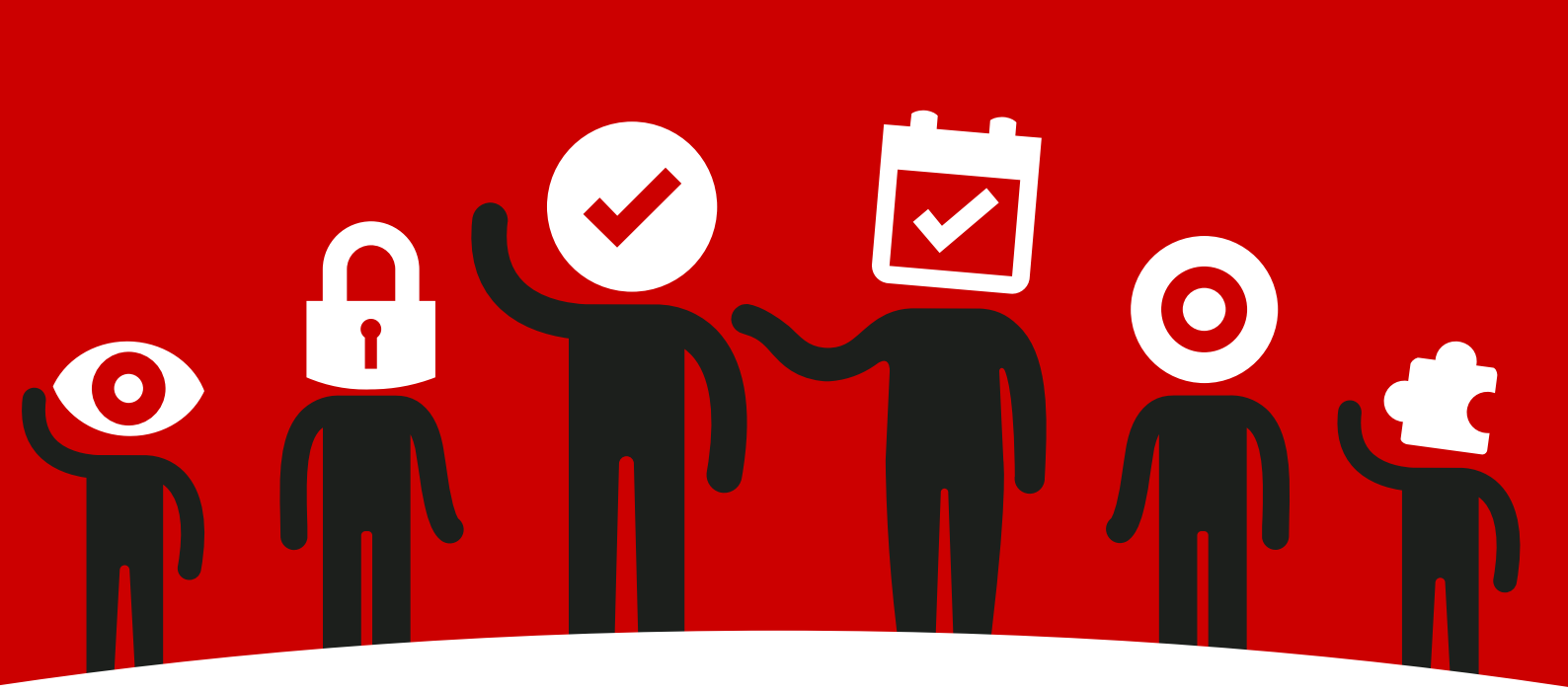

The GDPR

6 principles that impact SQL Server teams

redgate

The GDPR
6 principles that impact SQL Server teams

The EU's General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and will reshape the way organizations approach data privacy. It's not just for Europe either, as it places controls on any organization that handles EU citizens' personal data irrespective of where they're located.

The GDPR makes it essential for SQL Server teams to implement controls and processes for protecting personal data. But this doesn't mean you need to lock your data away or slow down your development processes.

Instead there are three practices to consider:

- Pseudonymize data in dev and test environments
- Maintain a data catalog of where you hold personal information
- Monitor for suspicious activity that could lead to a data breach

These best practices are guided by the following **six principles of the GDPR** that impact SQL Server teams.

GDPR Article 5 (1a)

"Personal data shall be processed lawfully, fairly and in a transparent

Lawfulness, fairness, and transparency

What this means for SQL Server teams

Data processing isn't just about data in transit, it also includes data at rest. You'll need to be clear on how the data will be stored, used, shared, and for how long. Clarity on processing will need to be defined up front in clear plain language when consent is given, and you'll need a record of this. Transparency is about knowing what data you hold, where, what is sensitive and what consent was given for use.

Processing needs should align to the necessity for the performance of a contract, because it's protecting the interests of the data subject or because it's in the public interest.

As a database team you'll need to know, for example, if consent was given to use data for development or testing, and the expectation around storage, profiling or sharing data with a third party. If this isn't a reasonable expectation in accordance with the processing needs, then teams should not be using the data, or they should find a way to de-sensitize PII data before use. Appropriate techniques for this may be to pseudonymize or anonymize data.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Estate Manager SQL Provision

Purpose limitation

GDPR Article 5 (1b)

"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes"manner in relation to the individuals"

What this means for SQL Server teams

You'll need to be clear on the purpose of collecting data and only process the data in accordance to the purpose outlined when consent was given.

Using PII data for a purpose beyond which it was collected should result in PII data being pseudonymized or anonymized prior to use.

For example, your development team might request a full copy of production to test a new application prior to release, however if data subjects haven't given consent for this use then you are not limiting processing and are expanding your attack surface area. This is where understanding the data you hold and having a process to pseudonymize or anonymize PII data as part of your development process will be key.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Provision

GDPR Article 5 (1c)

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"manner in relation to the individuals"

Data minimization

What this means for SQL Server teams

The data collected should be limited to the processing needs. Processing needs should align to the necessity for the performance of a contract, because it's protecting the interests of the data subject or because it's in the public interest. You should not be collecting additional data that isn't relevant to the processing need unless there's a legitimate purpose defined up front when consent is given for doing so.

Once the processing need is complete, you should be minimizing the data you hold. You should ensure your retention policy is clear and aligned with the processing need. This doesn't mean you need to delete all your data, but any PII data should be pseudonymized if you want to retain the data for additional use.

For example, if the need was to carry out a transaction and hold the data in case of a refund then your retention policy should align to the use of the data in order to fulfil performance of the contract, not to help with future troubleshooting, development or testing. In this case you may wish to keep data relating to the transaction but remove or pseudonymize PII data.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Provision SQL Backup Pro

Data accuracy

GDPR Article 5 (1d)

"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

What this means for SQL Server teams

Data subjects have a right to request for data you hold to be updated or 'rectified', and you have a limited time to ensure this is done. It's not only the data you hold but, as the controller, the data you share with processors.

If you don't know what data you hold, and how it's used or shared, then it's difficult to ensure data is kept up to date and respond to 'rectification requests' within a timely manner. This is where understanding the data you hold and how it is used or shared is critical. Again, limiting the use of PII data in other environments means limiting the surface area for rectification.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Estate Manager SQL Provision

Storage limitation

GDPR Article 5 (1e)

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals"

What this means for SQL Server teams

The storage of PII data should also be limited to the purposes for which the personal data was processed. Software teams should take measures to ensure the storage of PII data held in backups is aligned to the retention policy and clear consent is given to this upfront.

Organizations may also want to store data for another purpose such a business intelligence. In this case any PII data which hasn't been removed through aggregation should be pseudonymized.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Backup Pro SQL Provision

GDPR Article 5 (1f)

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures"

Integrity and confidentiality

What this means for SQL Server teams

Teams should have appropriate measures in place to protect data. This includes a process in place to identify a breach in a timely manner, understand why it occurred, who was affected and how to notify those data subjects. If you don't know what databases you have, what data is held within them, who has access and what 'normal' looks like then you cannot apply appropriate measures to ensure the integrity and confidentiality of them.

Equally you should be able to demonstrate compliance with all principles, so automation and documentation are key. It's not enough to say you are compliant, you must be able to prove it.

TOOLS THAT HELP YOU OBSERVE THIS PRINCIPLE

SQL Estate Manager SQL Provision SQL Monitor

Conclusion

GDPR compliance will be an evolutionary process for organizations, however from 25th May the ICO will be regulating and enforcing action on those who have not taken steps to get the appropriate systems and thinking in place.

Addressing the impact the 6 principles have on SQL Server teams is a great place to start. Redgate's tools help you maintain a GDPR compliant data catalog, pseudonymize data for non-production use such as development and testing, and monitor for emerging security risks.

Further reading

For more information and resources about data privacy and protection, visit red-gate.com/GDPR

The tools your team need

The **SQL Data Privacy Suite** helps you protect your business by providing a scalable and repeatable process for managing personal data as it moves through your SQL Server estate.

Our solution catalogs your SQL data estate and monitors and controls it for protection appropriate to the sensitivity of the data, ensuring compliance during data handling.

See the tools at red-gate.com/dataprivacysuite