6 Principles of the GDPR and SQL Provision
Your Presenter

Steve Jones
Evangelist, Redgate Software
Editor, SQLServerCentral

✉️ sjones@sqlservercentral.com
🐦 @way0utwest
🌐 www.voiceofthedba.com
.linkedin /in/way0utwest
Disclaimer

This is NOT legal advice

No legal review has been undertaken of this material

I am not a lawyer!
We will discuss

- 6 Principles of the GDPR
- Data compliance in software delivery
- How SQL Provision can help
The principles of GDPR are the principles of good data protection
Demonstrating Compliance

“In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default”
“Appropriate Technical Measures”

• Documentation

• Encryption, pseudonymization, anonymization

• Oversight of protection

• Change Control

• Procedures for out-of-process change
Accountability

“The controller shall be responsible for, and be able to demonstrate, compliance with the principles”

39 of the 99 GDPR Articles require evidence to demonstrate compliance
The 6 Principles
Lawful, fair and transparent

“Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals”

GDPR Article 5 (1a)
You should know what data you hold and what consent has been given ie what are the expectations around storage, profiling, using or sharing data?
Purpose Limitation

“Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”

GDPR Article 5 (1b)
If you are using data in multiple environments then you are expanding your attack surface area.
Data Minimisation

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

GDPR Article 5 (1c)
Remember your retention policy should align to the use of the data in order to fulfil the performance of the contract, not i.e. to help with future troubleshooting, development or testing.
Data Accuracy

“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”

GDPR Article 5 (1d)
Understanding the data you hold and how it is used or shared is critical.
"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."

GDPR Article 5 (1e)
If you wish you use the data for other purposes, such as business intelligence. PII data which hasn’t been removed through aggregation should be masked.
“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 organisational measures”

GDPR Article 5 (1f)
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.
Data Compliance in Software Delivery
Data Compliance in Software Delivery

1. What do you process?
2. What needs protecting?
3. Who has access and for what purpose?
4. How can you demonstrate adequate protection?
5. Are you monitoring for emerging security risks?

Move from tell me to show me...

...consistent processes are key
Most organizations do 'copy-down' live data

Where does the data in your development/test/QA environment come from? (multiple choice)

- A copy of production: 72%
- A modified copy of production (masked, subsetted, etc.): 50%
- Synthesized: 13%
- Manually created: 28%

What Compliant Provisioning Looks Like

• Single central view of database copies
• Control over creation and access
• Mechanism to protect data classified as sensitive
• Consistent (automated) process are easier to audit
• Record of activities
Conflicts around the use of data

Teams want to move fast
- up-to-date, realistic data
- on-demand access to consistent database copies

DBAs must protect data
- all copies of data accounted for
- sensitive data must be sanitized
SQL Provision: Create, protect and manage provisioning
Demo
Key Benefits

**Virtualize**
- Save time provisioning
- Save 99% storage space
- Local, isolated development
- Accurate testing using realistic data

**Protect**
- Mask sensitive data for compliance
- Customize data masking rules at scale

**Automate**
- Automate repeatable processes
- Fewer provisioning requests

**Manage**
- Central auditable view of database copies
- Role-based provisioning permissions
The best compliance is deterministic

- It’s not that you ‘did the right thing’
- It’s that ‘the right thing is ALWAYS done’

The use of data should be driven by the consent given and the processing policies agreed to. Behaviours of its use is then driven by its classification.
Need help?

Contact Us:

- sales@red-gate.com
- sqlprovision@red-gate.com

Discover Redgate’s Full Solution

Data Privacy and Protection
www.red-gate.com/solutions/data-privacy-protection

SQL Data Privacy Suite