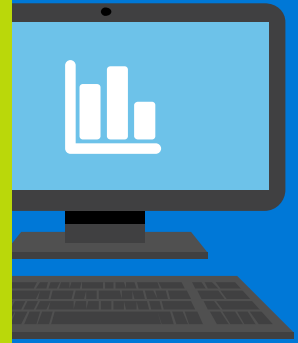




Quiz

How does GDPR impact your business?

Effective May 25, 2018, the General Data Protection Regulation (GDPR) introduces new requirements about how organizations manage and protect personal data while respecting individual choice—no matter where the data is sent, processed, or stored. Take this 10-question quiz to check your knowledge about the GDPR and what it means for your organization.



1. Does the GDPR apply to my organization?

- ▶ Impacts organizations that offer goods and services to people in EU or collect and analyze data tied to EU residents, no matter where they are
- ▶ Includes companies, government agencies, non-profits, and others
- ▶ For all sizes of organizations: small, large, and enterprise

● Pro Tip:

The GDPR isn't just Europe – it applies more broadly than many people think.

2. Is the data my organization processes subject to the GDPR?

- ▶ GDPR regulates collection, storage, use, and sharing of "personal data"
- ▶ Includes any data related to an identified or identifiable person
- ▶ Personal Identifiable Information (PII)
- ▶ Some identifiers: IP address, employee information, sales data, customer data, and biometric data



● Pro Tip:

The GDPR is all about personal data, which can reside in:

- Customer databases
- Feedback forms filled out by customers
- Email content
- Photos
- CCTV footage
- Loyalty program records
- HR databases

3. What are the risks if we don't comply?

- ▶ Fines can be up to 4% of annual turnover or €20 million
- ▶ Individuals (or organizations acting on their behalf) can start civil litigation
- ▶ Other organizations may only work with you if you're compliant



● Pro Tip:

Up until now, data protection laws did not include significant fines. The GDPR changes things dramatically. GDPR compliance is not a one-time activity and carries significant penalties for non-compliance.

4. What are the main requirements?

- ▶ Transparency, fairness, lawfulness when handling and using personal data
- ▶ Data processing minimization
- ▶ Collection and storage minimization
- ▶ Ensure accuracy of personal data
- ▶ Limit storage
- ▶ Ensure security, integrity, and confidentiality



● Pro Tip:

Organizations need to be clear how they handle personal data – there must be a lawful basis. Processing is limited to specified, explicit, legitimate purposes. Storage should be adequate and relevant for the intended purpose.

5. What does transparency really mean?

- ▶ Organizations must tell individuals about their data processing
- ▶ Why it is processed, how long it is stored, with whom it is shared, and is it transferred outside the EU
- ▶ Easy to access and understand format



● Pro Tip:

Data controllers must ensure that anyone whose data is collected is kept adequately and sufficiently informed about just what is being done, and will be done, with their data.

6. What are some of the other requirements?

- ▶ Implement privacy by design and privacy by default
- ▶ Appoint a Data Protection Officer
- ▶ Institute data breach reporting



● Pro Tip:

The Data Protection Officer should be accountable to the highest level to ensure compliance. The data breach reporting threshold is lower under GDPR.

7. What are individual rights?

- ▶ Access to personal data an organization holds for an individual
- ▶ Right to be forgotten
- ▶ Stop processing, revoke consent, and data portability



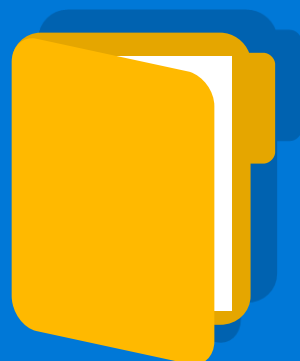
● Pro Tip:

The GDPR was designed to strengthen the rights of EU citizens and does so by clarifying, extending, and introducing new rights.

8. What kind of record keeping is required?

Organizations need to maintain detailed processing records

- ▶ Purpose of processing
- ▶ Data categories processed
- ▶ Data transfers
- ▶ Security measures employed



● Pro Tip:

The GDPR sets new standards in record-keeping. Organizations processing personal data will need to keep detailed records to be compliant.

9. What if a data breach occurs?

- ▶ Data breach includes accidental destruction, loss or alteration of personal data or unauthorized disclosure of personal data
- ▶ Obligation to notify regulator and/or consumers within 72 hours



● Pro Tip:

The GDPR requires organizations take appropriate measures to prevent unauthorized access or disclosure and to notify stakeholders in the case of breach.

10. Can Microsoft help us meet the GDPR requirements?

- ▶ Yes! Microsoft is adding technology, documentation, capabilities, and transparency to help organizations with GDPR compliance
- ▶ [Microsoft has committed to Enterprise Online services compliance by May 2018](#)



● Pro Tip:

GDPR analysis begins with understanding what data exists and where it resides, and taking appropriate steps. As a Microsoft partner, we can work with you to help you make the most of available tools and technologies.

Make sure you're prepared to meet and stay compliant with the GDPR.

It's not surprising if your answers to this simple GDPR quiz have made you reconsider your approach to the GDPR – this new regulation will typically require making changes to people, processes, and technology. Contact us to learn how capabilities in Microsoft 365 and our services can help.

Email: Info@cubesys.com.au

Web: <http://www.cubesys.com.au/services/GDPR>

