bakertilly
now, for tomorrow.

Your GDPR primer

What is GDPR? To whom does it apply?

The General Data Protection Regulation (GDPR) is the European Union (EU) regulation governing the collection, processing, use and storage of any individual's personal data originating in the EU (citizens, residents and visitors as well as EU citizens living abroad). It applies to all organizations, including U.S.–based companies.

Impacts of non-compliance are significant

Financial: Fines of up to 4 percent of annual global revenue or €20 million (whichever is greater).

Material and non-material damages: For example, discrimination, financial loss, damage to reputation, etc.

Legal: Individuals can choose to sue either the data controller or the processor, or both, and possibly anyone in the supply chain.

What data is covered?

- Basic identity
- Web (e.g., IP address, cookie data)
- Health and genetic
- Biometric
- Mental
- Cultural
- Economic
- Social and political identity

Key terms and concepts

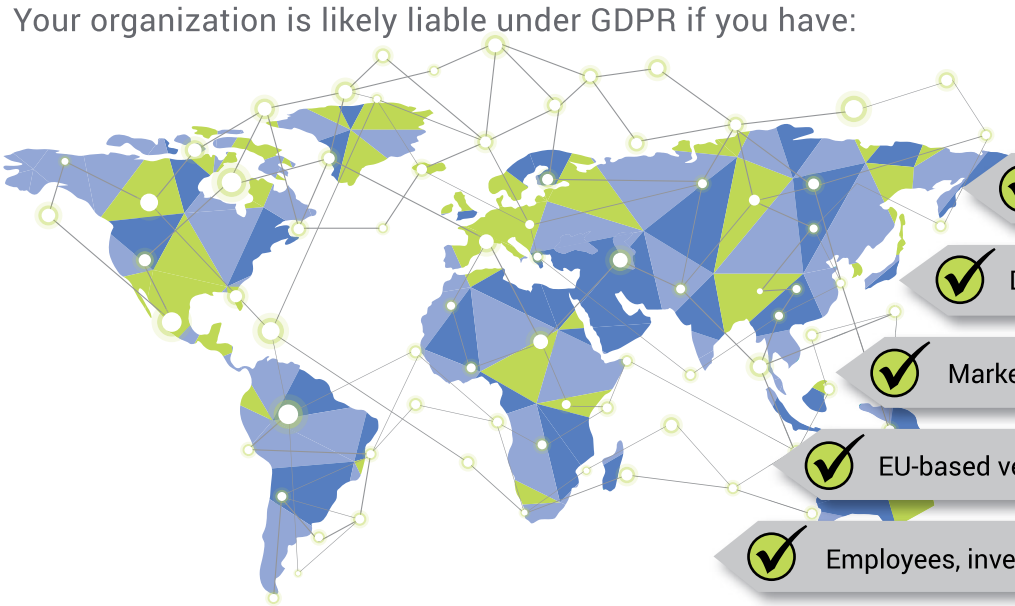
Data minimization – Limit personal data collection, storage and usage to data that is relevant, adequate and necessary in carrying out the reason for which the data was processed

Right to be forgotten – Provide individuals the right to have their personal data erased and to prevent further processing in certain circumstances

Privacy by design and privacy by default – Incorporate data privacy into the design of all projects as well as the entire lifecycle of the data

What is your GDPR footprint?

Your organization is likely liable under GDPR if you have:



- A presence in the EU
- Customers/clients in the EU
- EU suppliers
- Data-related businesses
- Marketing efforts in the EU
- EU-based vendors
- Employees, investors or customers who are EU citizens

What to do now

- Engage senior leadership in setting the tone at the top of your organization and establishing a sense of urgency
- Involve relevant stakeholders
- Evaluate your current cybersecurity and privacy program
- Consult legal counsel
- Implement risk-based compliance monitoring measures

Connect with us:

bakertilly.com/GDPR

Baker Tilly Virchow Krause, LLP

@bakertillyUS