

The EU Data Act – Privacy Friend or Foe?

David Cox

Assistant General Counsel - Privacy, Data
Governance & E-Discovery, Volkswagen of America

Briony Pollard

Willkie Farr & Gallagher (UK) LLP

Laura E. Jehl

Willkie Farr & Gallagher LLP

Speakers



David Cox

Assistant General Counsel –
Privacy, Data Governance & E-
Discovery
Volkswagen of America



Laura E. Jehl

Partner and Co-Chair,
Privacy, Cybersecurity & Data
Strategy
Willkie Farr & Gallagher LLP



Briony Pollard

Partner, Privacy,
Cybersecurity & Data Strategy
Willkie Farr & Gallagher (UK) LLP

EU Data Act

The Basics:

- Background
- Scope
- Extraterritorial Effect
- Key Provisions
- Effective Dates

2020: EU Commission launches EU data strategy

- Goal to create a single market for data within the EU
- Support competitiveness and digital sovereignty, remove barriers to data sharing, create fairness, improve switching between service providers
- To promote horizontal data sharing (personal and non-personal data) related to connected products and services in the market
- Establishes data sharing obligations in B2C, B2B, and B2G relationships

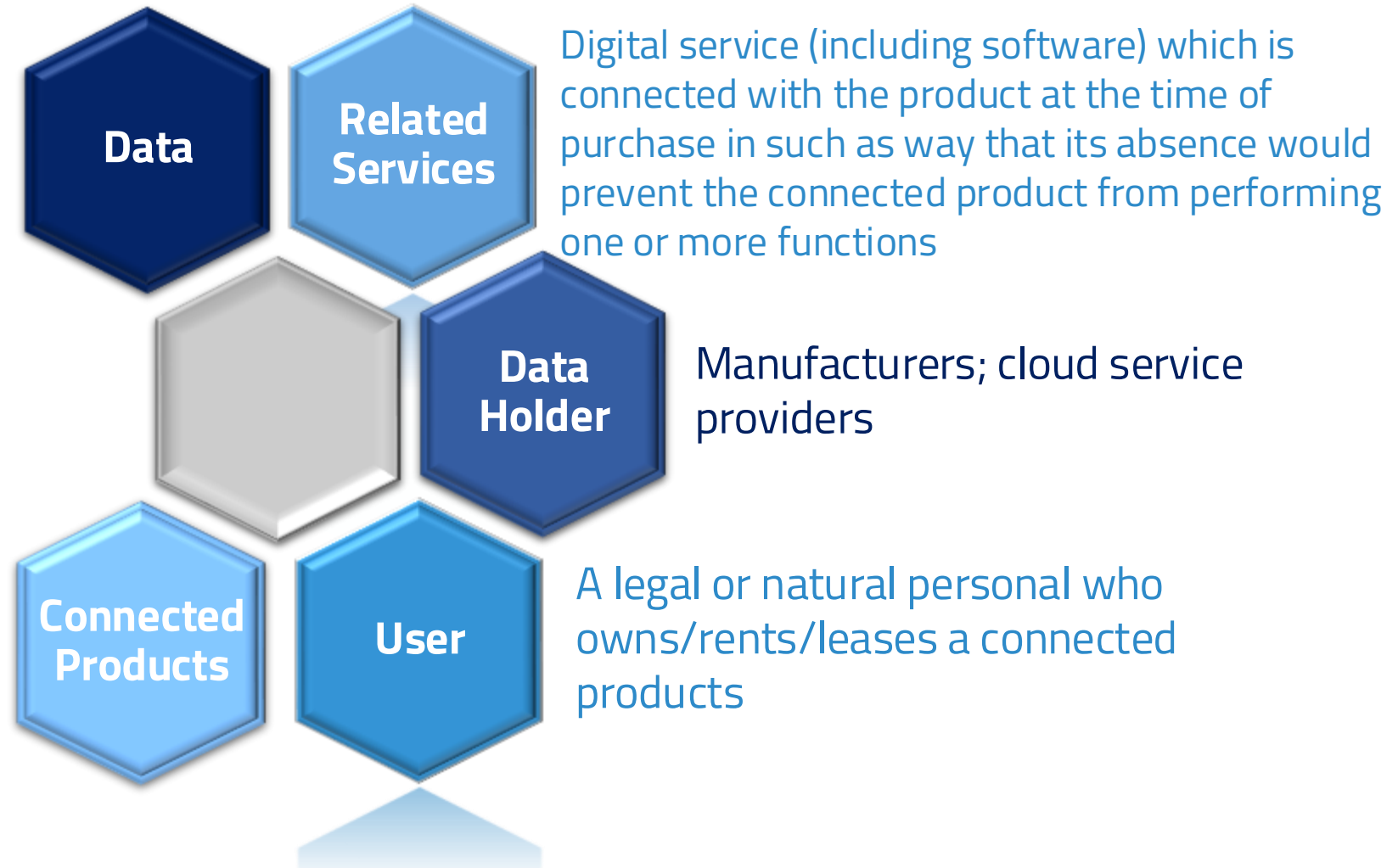
THE BASICS: SCOPE

Personal and non-personal data generated by products and related services (raw data included; derived or inferred data excluded)

Items that can generate, obtain, or collect data about their use, performance, or environment and that can communicate product data via a cable-based or wireless connection

Connected products within scope if *'placed on the market in the EU'*

Examples: **smart products, such as health wearables; home assistant devices; vehicles; washing machines; farm machinery**



THE BASICS: EXTRATERRITORIAL EFFECT

EU law, but applies to organizations outside of the EU

1

Manufacturers of connected products placed on the market in the EU and providers of related services

2

Providers of data processing services, providing services to customers in the EU

3

Both irrespective of the place of establishment of the manufacturer/provider

THE BASICS: KEY PROVISIONS

Interoperability

- increased interoperability through data sharing agreements

User Rights

- users can request data sharing with third parties

Switching Providers

- reduce barriers so that customers are able to easily switch between providers

Unfair Contractual Terms

- list of unfair or presumed unfair terms

B2B Data Sharing

- fair, reasonable, and non-discriminatory terms required

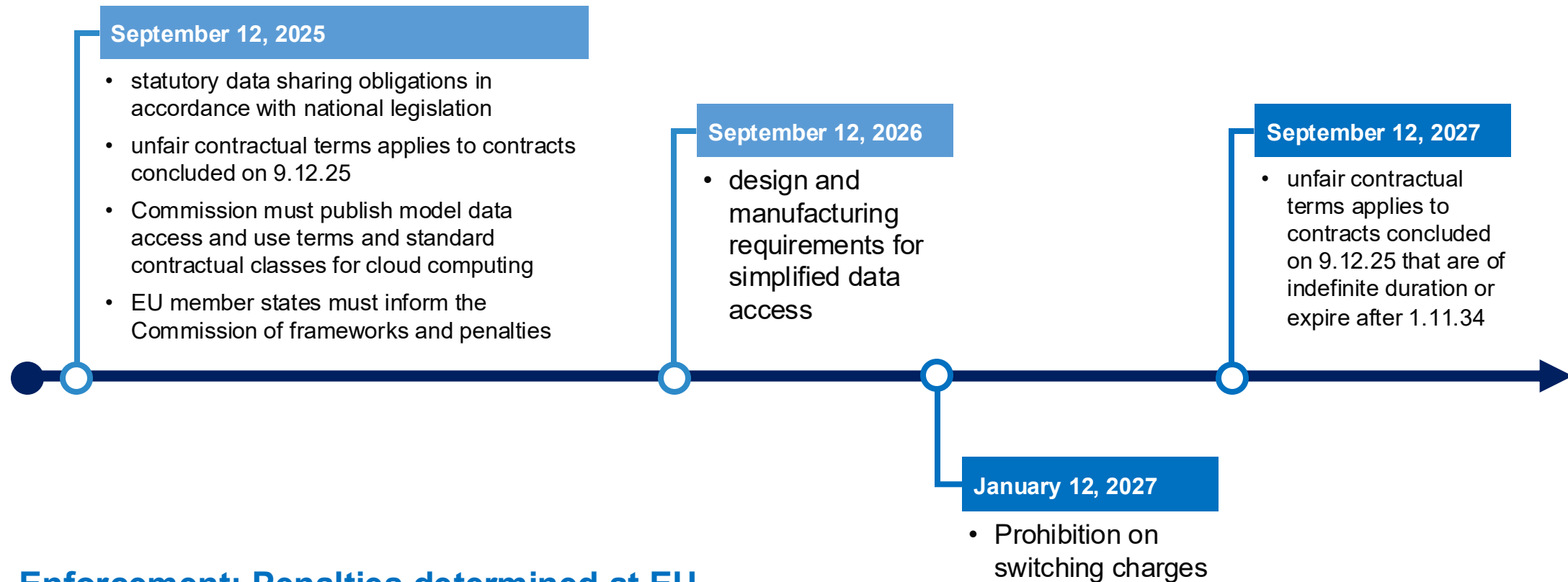
B2G Data Sharing

- sharing with public sector allowed for 'exceptional need' situations

Governmental Requests

- access requests or transfers of non-personal data from the EU to third countries must include safeguards

THE BASICS: EFFECTIVE DATES



Enforcement: Penalties determined at EU member state level; up to €20 M or 4% global annual turnover if personal data violation

CONNECTED PRODUCTS



EU Data Act

- Overlap with the GDPR
- Supremacy of Data Protection Laws
- Identifying Personal Data
- Examples of Connected Products
- Data Access Requests
- Valid Legal Basis
- Transparency Requirements

OVERLAP WITH THE GDPR



EU Data Act

- Aim is to open up digital economy by providing incentives and removing disincentives from data sharing both B2B and B2C
- Impacts activities that create and hold substantial amounts of data i.e. connected products/services and cloud services
- Captures personal and non-personal data



GDPR

- Aim is protect and safeguard personal data and individuals' right to privacy
- Applies to anyone processing EU/UK personal data
- Limited to personal data

SUPREMACY OF DATA PROTECTION LAWS

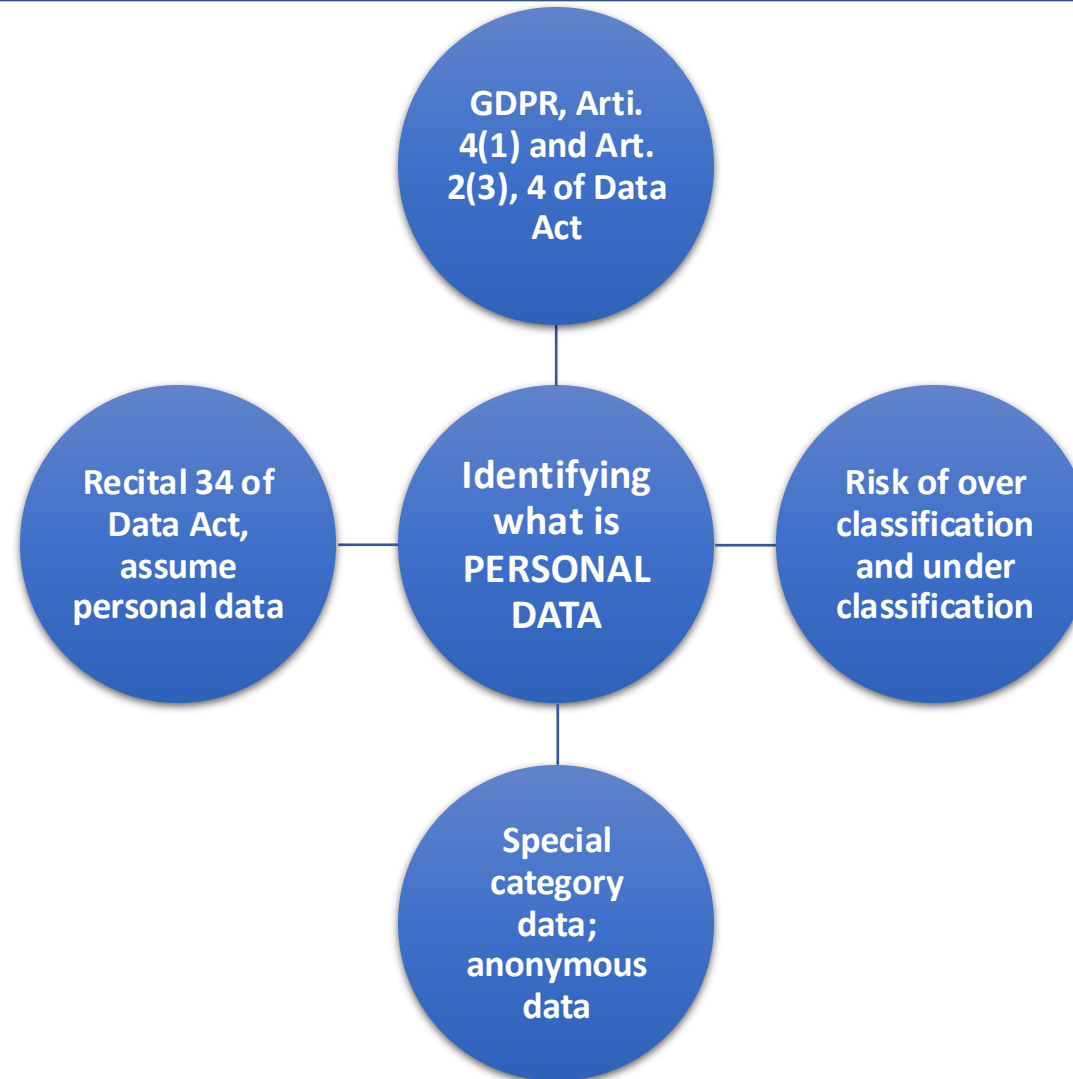
Data Act reaffirms the supremacy of data protection laws

Article 1(5)/Recital 7 - Data Act is “without prejudice to” the GDPR

In the event of a conflict between the Data Act and the GDPR, the GDPR shall prevail

EU Commission FAQ 3 February 2025: *“The GDPR is fully applicable to all personal data processing activities under the Data Act. The Data Act does not regulate as such the protection of personal data.”*

IDENTIFYING PERSONAL DATA



DATA ACCESS REQUESTS

EU DATA ACT	GDPR
<p>Connected product data accessibility requirement that a data holder provide the user with continuous and real-time (where feasible) access to generated data</p> <p>Users' right to have their data being made available to a third party of their choice</p>	<p>GDPR requires controllers to provide a copy of the personal data it holds relating to a data subject on request</p> <p>Data portability request</p>
<p>Request can relate to all generated data - personal data unrelated to the product is not in scope</p> <ul style="list-style-type: none">Exemptions e.g., trade secrets hand break; security hand break	<p>Request should be limited to personal data - only a snapshot of what is held at the time of the request</p> <ul style="list-style-type: none">Exemptions e.g., management forecasting and planning
<p>Timelines for response – ‘without undue delay’. Data should be made available in a ‘prompt, timely and responsive manner’</p>	<p>Timelines for response – one calendar month (subject to two months’ extension)</p>
<p>Verification of requester requirements – Recital 29 ‘data holders may require appropriate user identification to verify a user’s entitlement to access the data’</p>	<p>Verification of requester identity – Recital 64 ‘controller should use all reasonable measures to verify the identity of a data subject who requests access’</p>

VALID LEGAL BASIS FOR PROCESSING

Personal data can be provided if either:

- a) the user is the data subject to whom the personal data relates, or
- b) there is a valid legal basis under the GDPR for processing

User and data subject may not be the same

Data Act itself explicitly does not justify processing of personal data; therefore the Article 6/9 GDPR legal bases apply

Which legal basis is most appropriate?

- Art. 6(1)(f) – legitimate interest
- What does a data holder need to do to apply the legal basis?

TRANSPARENCY REQUIREMENTS

EU DATA ACT

Cloud switching requirements include providers informing customers, via a website, how to switch services

Connected product data accessibility obligations require pre-contractual information be provided to users, including the types of data the product generates, how long it will be kept and how it can be accessed

Sufficient that information is provided in a *“clear and comprehensible manner”*

GDPR

Data subjects must be provided with information about the purpose and nature of the processing of their personal data

Higher standard - information has to be provided in a *“concise, transparent, intelligible and easily accessible form, using clear and plain language”*

EU Data Act

Questions?

Contacts



David Cox

David.Cox@vw.com



Laura E. Jehl

Ljehl@willkie.com

(202) 303-1056



Briony Pollard

bpollard@willkie.com

(44) 203-580-4716