October 24, 2024

EU Data Act

The Key Issues Privacy and IP Lawyers Should Consider

Lynn Parker Dupree
Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Naim Surgeon
NextEra Energy Resources

Nicole Beranek Zanon
HARTING Attorneys at Law Ltd.

Privacy+
Security
Forum

Speakers

Privacy+ Security Forum

Lynn Parker Dupree
Partner
Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Naim Surgeon
Managing Attorney
NextEra Energy Resources

Nicole Beranek Zanon
Lic. Iur., Exec.MBA HSG
HARTING Attorneys at Law Ltd.

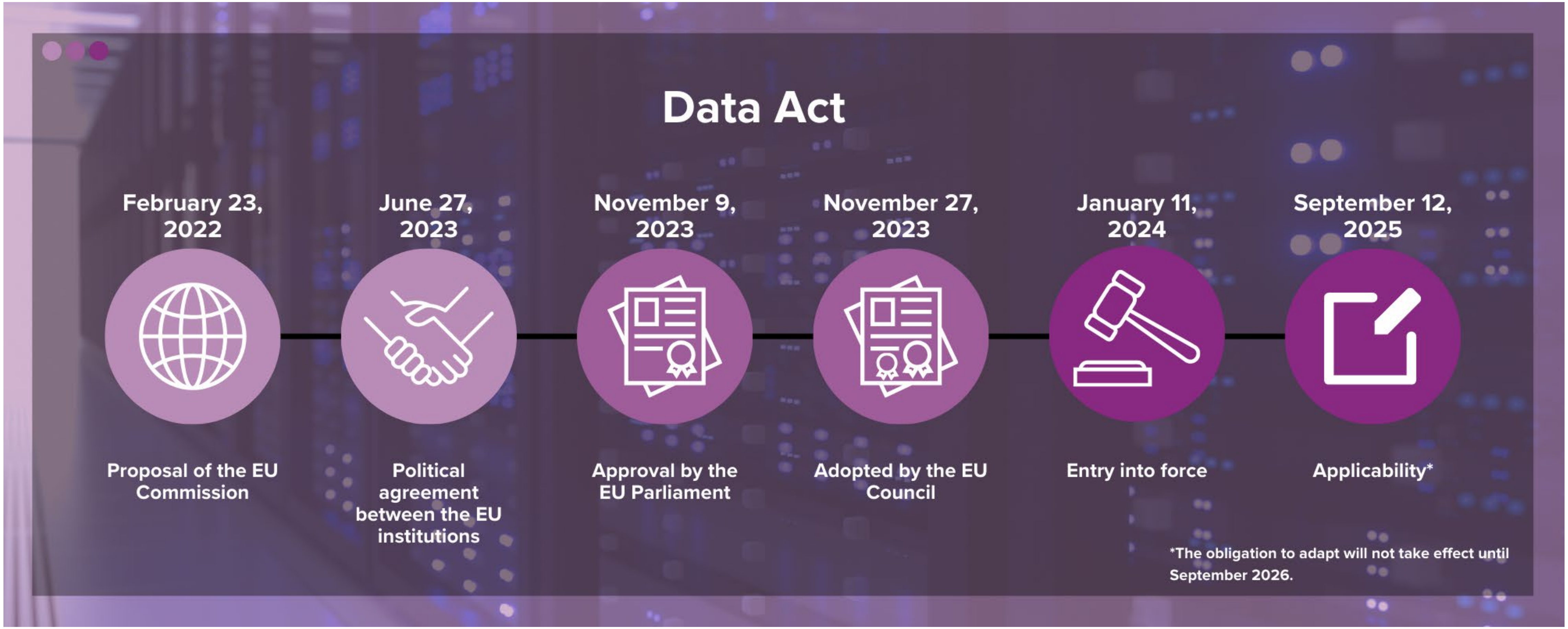
Presentation Overview

1. Overview of the EU Data Act
2. Categories in the Law
3. IP Challenges
4. Open Questions
5. Compliance Approach
6. Closing and Questions

Objectives & Applicability

Nicole Beranek Zanon

From proposal to EU-wide data law



Data Act

February 23, 2022
Proposal of the EU Commission

June 27, 2023
Political agreement between the EU institutions

November 9, 2023
Approval by the EU Parliament

November 27, 2023
Adopted by the EU Council

January 11, 2024
Entry into force

September 12, 2025
Applicability*

*The obligation to adapt will not take effect until September 2026.

Primary objectives Art. 1 Sec. 1. DA

- Data access right of product data and related service data to users and other data recipients
- Making available data to public authorities in cases of exceptional need for the public interest
- Switching between data processing services
- Introducing standards for data interoperability to be accessed, transferred and used
- Safeguards against unlawful third-party access to non-personal data

⇨
- Facilitate data sharing in relation to connected devices
- Reduce competitive barriers

Scope of the Act – personal and non personal data Art. 1 Sec. 2 DA

The DA covers personal and non-personal data and applies especially to:

- data, with the exception of content, concerning the performance, use and environment of connected products and related services;
- any private sector data that is subject to statutory data sharing obligations;
- any private sector data accessed and used on the basis of contract between enterprises;
- any private sector data with a focus on non-personal data;
- any data and services processed by providers of data processing services;
- any non-personal data held in the Union by providers of data processing services.

Personal Applicability of the Data Act Art. 1 Sec. 3 DA

(a) manufacturers of connected products placed in the EU market and providers of related services

(b) users in the Union of connected products or related services as referred to in point (a);

(c) data holders, that make data available to data recipients in the Union;

(d) data recipients in the Union to whom data are made available;

(e) public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;

(f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;

(g)participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

Para. 4 virtual assistants insofar as they interact with a connected product or related service

Applicability of the Data Act (2/2)

- **Manufacturer of networked products**
  - **object that obtains, generates or collects data about its use or environment and**
  - **can transmit product data electronically or via a physical connection and**
  - **whose main function is not data storage.**

- **Exceptions**
  - **Small businesses and micro-enterprises**
  - **Medium-sized companies (cumulative):**
    - **Number of employees is < 250 and**
    - **Turnover < 50 million**
    - **Product placed on the market less than one year**

Use Case (1/3)

- Robot vacuum cleaners are networked products:
  - ✓ Physical object
  - ✓ Collection, generation or receipt of data on its use
  - ✓ Ability to transmit product data electronically

- Manufacturers are generally not small companies

Use Case (2/3)

- **Wind turbines are networked products:**
  - ✓ Physical object
  - ✓ Collection, generation or receipt of data on its use
  - ✓ Ability to transmit product data electronically

- **Manufacturers generally not small companies**

Use Case (3/3)

- John Deere tractors are networked products:
  - ✓ Physical object
  - ✓ Collection, generation or receipt of data on its use
  - ✓ Ability to transmit product data electronically

- Manufacturer is not a small company

Key Terms Defined

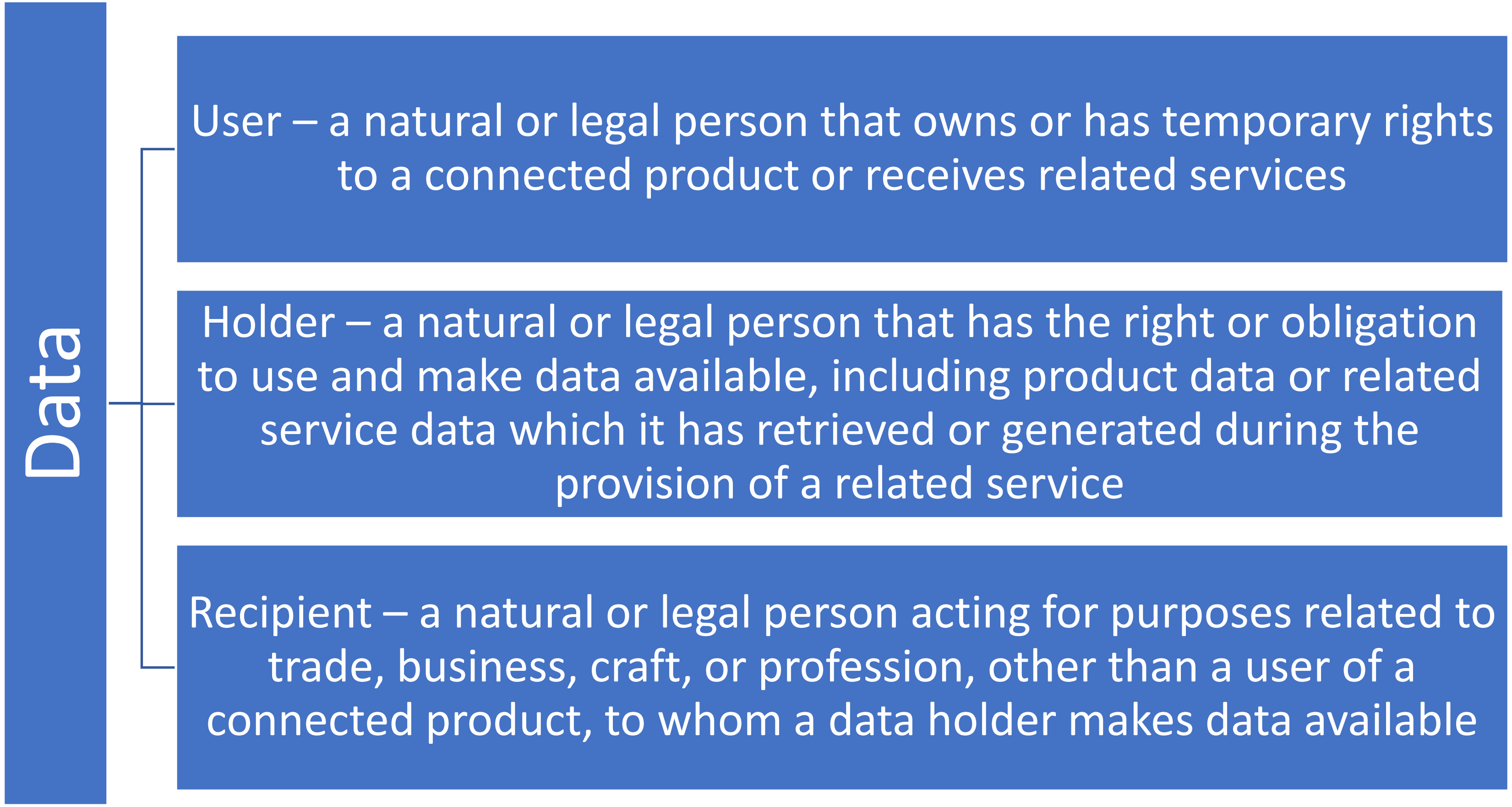
Naim Surgeon

Privacy+ Security Forum

Key Terms Defined

Product Data – Data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including the manufacturer

- **Data Act parties of interest**
  - **User**
  - **Data Holder**
  - **Data recipient**



Data

User – a natural or legal person that owns or has temporary rights to a connected product or receives related services

Holder – a natural or legal person that has the right or obligation to use and make data available, including product data or related service data which it has retrieved or generated during the provision of a related service

Recipient – a natural or legal person acting for purposes related to trade, business, craft, or profession, other than a user of a connected product, to whom a data holder makes data available

Categories in the Law

Lynn Parker Dupree
Naim Surgeon
Nicole Beranek Zanon

B2C: Users are granted access rights to the data

- Users of the networked product have the right to access data
  - User within the meaning of Art. 2 No. 12 DA
    - Natural or legal person,
    - which has a networked product or,
    - to which temporary rights to use the networked product have been contractually assigned.
- Owner is not automatically user
  - Right of access therefore also applies to leasing or acceptance from third parties
- User (or de facto user) not necessarily a user within the meaning of the Data Act

B2B: Data use by the manufacturer subject to reservation

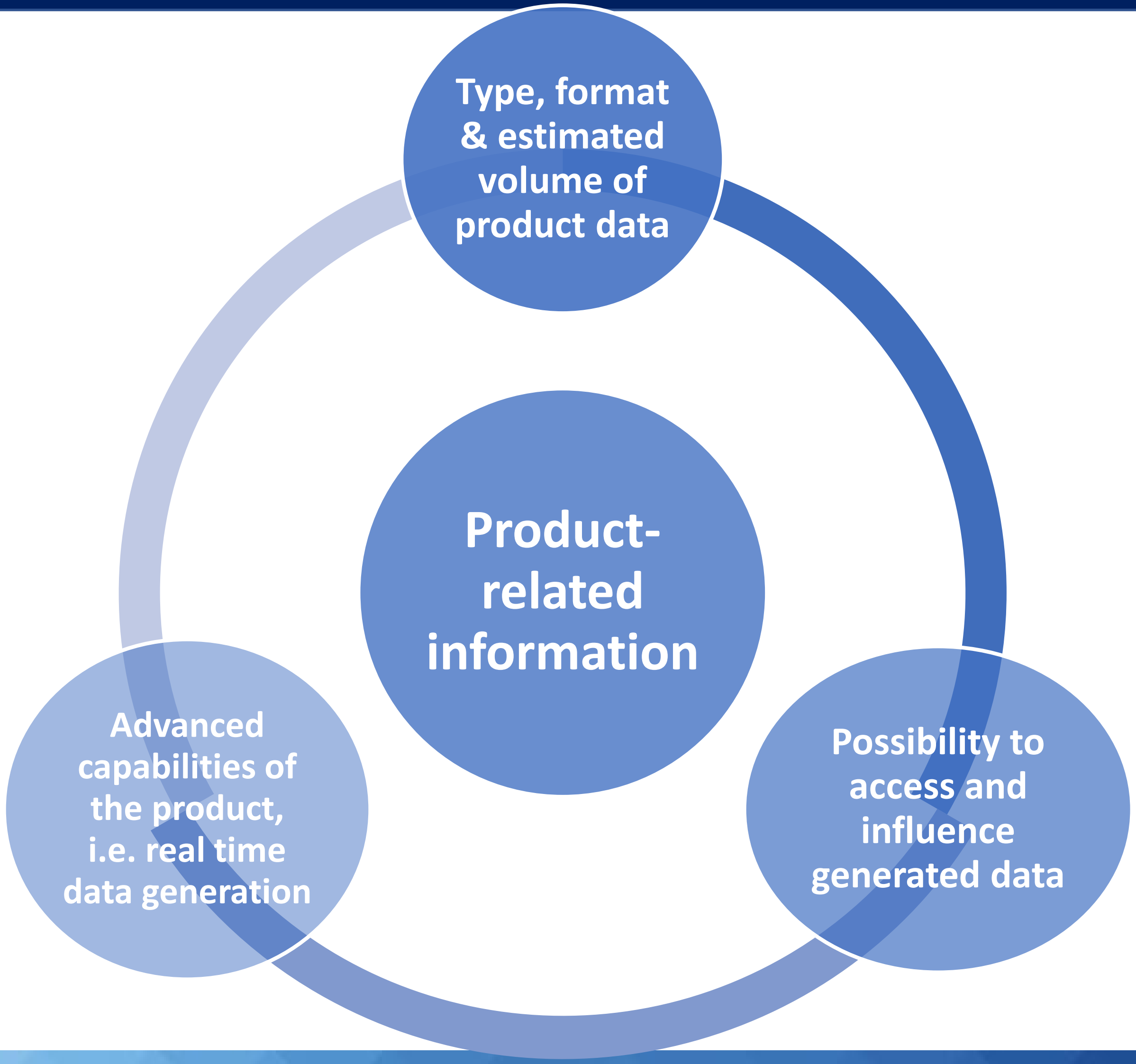
- Relationship between users and manufacturers will change
- The user has the right to the generated data
  - Manufacturers must make this data available free of charge
  - No more (chargeable) bonus feature
- Manufacturers need an independent legal basis for using data for their own purposes
  - For non-personal data: Data license agreements
  - For personal data: Art. 6 para. 1 sentence 1 GDPR
  - Without such a basis, further use (and disclosure to third parties) is prohibited

Subject of the duty to inform

Privacy+ Security Forum

- Product-related information
  - Type, format and estimated volume of product data
  - Advanced capabilities of the product:
    - Continuous and real-time data generation
    - Storage on the device or on a server, including storage duration
  - Possibility to access and influence generated data
- Information on asserting the right of access to data
  - Identity of the data owner
  - Exact purpose of use (own purpose/ third party use)
  - Contact information of the data owner
  - Procedure for requesting the sharing of data with third parties
  - Right of appeal

Subject of the duty to inform (1/2)



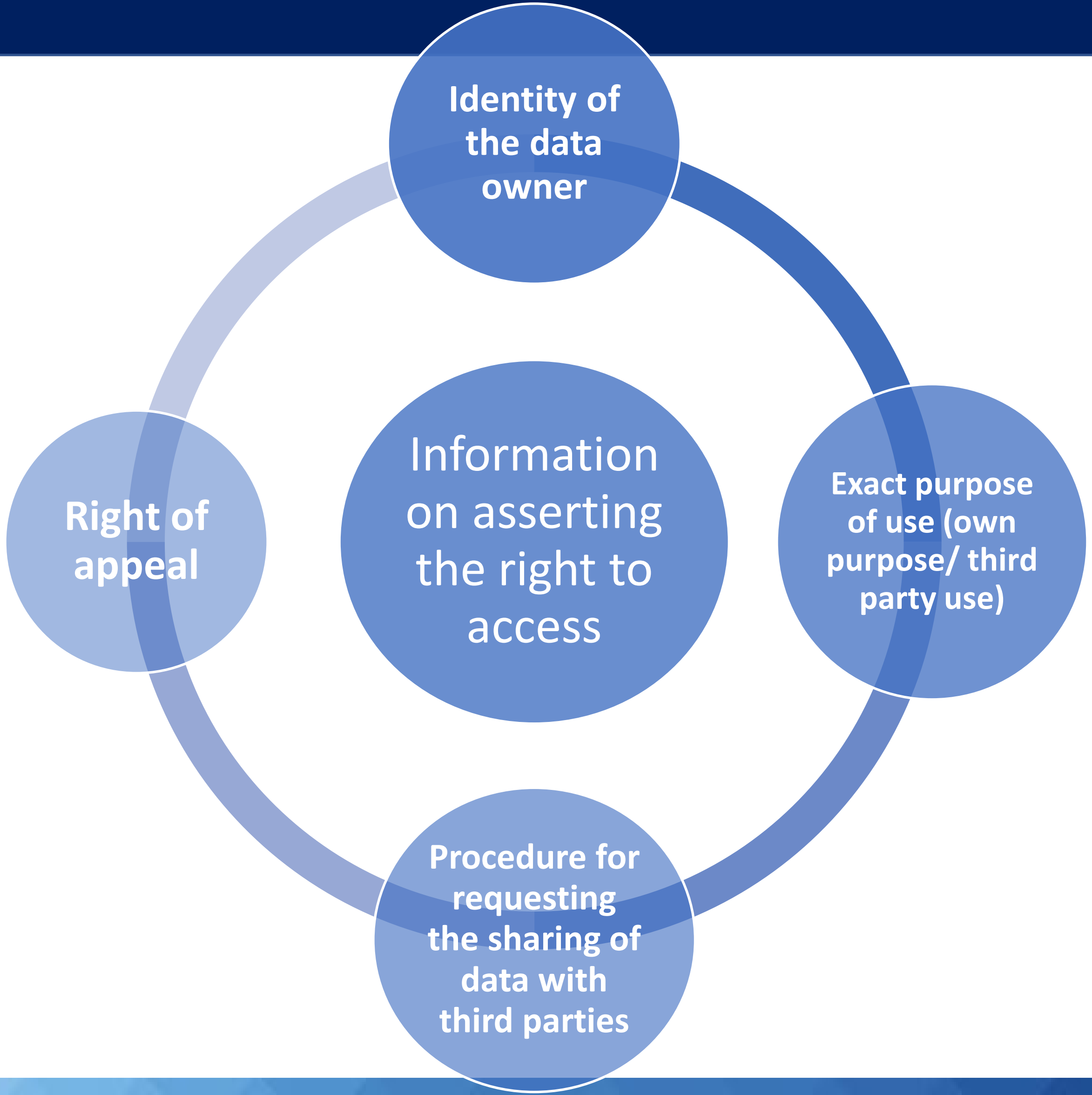
Type, format & estimated volume of product data

Product-related information

Advanced capabilities of the product, i.e. real time data generation

Possibility to access and influence generated data

Subject of the duty to inform (2/2)



Information on asserting the right to access

Identity of the data owner

Exact purpose of use (own purpose/ third party use)

Procedure for requesting the sharing of data with third parties

Right of appeal

Business to Government (B2G)

- The Data Act requires that businesses share all necessary data with the government in times of exceptional need at no charge to the government. This includes non-emergency and public emergency situations.
  - Public emergencies include:
    - Natural disasters
      - Ex: user location information during national disaster
    - Public Health crises
      - Ex: disease outbreak tracking data
    - Human-caused emergencies
      - Ex: Data produced related to infrastructural power outage
    - National Security Incidents
      - Ex: General cybersecurity-related user information
  - Non-emergency data
    - Ex: Aggregated GPS data for traffic flow optimization

Natural disasters (hurricanes, tornadoes, wildfires, floods, earthquakes)

Emerging or significant outbreaks of diseases (COVID-19, Pandemic Influenza)

Human-caused disasters (bioterrorist attacks, nuclear/radiation accidents)

Business to Government (cont.)

- B2G data disclosure requirements may raise cybersecurity concerns, namely potential program insecurities
  - The Data Act tries to combat this concern by:
    - Limiting the governments use of the provided data only to purposes required in the initially intended use
    - Limiting multiple government requests for the same data (“once only policy”)
    - Introducing safeguards that prevent government bodies from third countries from accessing data that would go against EU or national law.
  - Data Holders can also combat these concerns by:
    - Declining or avoiding requests for non-emergency data
    - Increasing safety measures to prevent unintended access to data
    - Declining data sharing that would undermine security requirements of a product, resulting in serious adverse effects to the health, safety, or security of people

Data Holders Rights

- Data holders still maintain rights. These rights include:
  - The right to withhold trade secret information
  - The right to withhold data that could undermine security requirements
  - The right to restrict access to third parties or users that will develop competing products

IP Challenges

Lynn Parker Dupree

Trade Secret Protection Requirements

- **Under the Act, users can request trade secrets be disclosed where the user and data holder align on confidentiality preservation measures.**
  - Trade secret holders can reject request if they demonstrate that there is a high likelihood of suffering "serious economic damage from the disclosure of trade secrets, despite the technical and organizational measures taken by the user
  - Trade secret holders can refuse access to data on a case by case basis by demonstrating:
    - Enforceability of trade secrets protection in third countries;
    - Nature and level of confidentiality of the data; and
    - The uniqueness and novelty of the connected product to users and authorities in a timely manner.
  - To avoid and overcoming potential challenges to trade secret disclosure requests, IP holders should consider taking the following actions:
    - Update business processes to ensure alignment with the Act
    - Preemptively consider legal arguments to support maintenance of trade secret confidentiality.

EU Data Act harmony with GDPR

Lynn Parker Dupree
Naim Surgeon
Nicole Beranek Zanon

Privacy+ Security Forum

Coexistence of the Data Act and GDPR

- Art. 1 para. 5 DA: Provisions of the Data Act should be applicable in addition to provisions of data protection law and have no prejudice over GDPR, GDPR prevails
  - Responsibilities of the supervisory authorities remain unaffected
  - Rights of data subjects remain unaffected
  - Provisions of the Data Act should not be interpreted in a way that weakens or restricts data protection (see recital 7 DA)
  - Impairment of the level of data protection should be avoided
- User rights under the Data Act are intended to supplement the rights of data subjects under the GDPR
  - In addition to Art. 15 (right of access) and Art. 20 GDPR (right to data portability), you have the right under the DA to
  - User under the Data Act may be a data subject under the GDPR
- Users under the Data Act may be a data subjects under the GDPR (B2C)
- Triangular constellations:
  - Affected parties are employees of the user
  - several affected persons use the product
  - Affected parties can be contractual partners of the user and use networked products
  - Affected parties can also use a networked product without a contract
- Personal reference on the manufacturer side?

Rights of use of the data owner

Personal Data	Non-Personal Data	Partial Personal Data
No license requirement	Provisions of the Data Act apply → License agreement required	“Inseparably" mixed data or personal reference unclear
Use is based on the requirements of the GDPR		With regards to non-personal elements: Consider license requirement
Problem: Differentiation between personal data and non-personal data -> Correct qualification is more important		Regarding the entire data set: Observe the provisions of the GDPR

Data access rights of the user

- **If data is to be provided = personal data:**
  - Legal basis required in accordance with Art. 6, 9 GDPR
    - Important: The Data Act itself is not a legal basis pursuant to Art. 6 para. 1 lit. c GDPR
  - suitable proof of user status (cf. Art. 11 para. 2 GDPR)

- **Problem: Disconnection between the user and user data**
  - Example 1: Employee uses networked product
  - Example 2: Majority of people use networked product (shared flat/ family/ second buyer)
  - Example 3: Third parties use networked product

Legal basis for granting access

- **Unproblematic: if user = affected person**
- **Problem if user ≠ user (affected party)**
  - Consent of the data subject
    1. towards users
    2. towards manufacturer
  - **In the employment relationship: work agreement as a legal basis?**
  - **Necessity for the performance of a contract with the data subject? (-)**
  - **Necessity to fulfill a legal obligation? as a rule (-)**
  - **Justified interest?**
    - Ensuring fair access to data = Legitimate interest? → Could again contradict Recital 7 DA
    - Weighing of interests

Right to anonymization before transmission?

- Anonymization makes legal basis from GDPR unnecessary
  - explicitly mentioned in recital 7 DA
- But: Art. 2 No. 17 "Readily available data"
  - "Product data [...] which a data controller lawfully [...] obtains or can obtain without disproportionate effort [...]"
  - Successful anonymization of data requires considerable legal and technical prerequisites
  - In addition: Anonymization = processing of personal data → Again requires a legal basis

Interim conclusion

- Significant potential for errors in both directions
    - Incorrect classification of the data as personal:
        - Refusal of data access request may constitute a breach of the Data Act
    - Incorrect classification of the data as non-personal:
        - Disclosure of data may constitute a breach of the GDPR
- It is often not clear whether the data is personal or not
    - Indirect personal reference possible
- Increased liability risks for the data controller

Open Questions

Naim Surgeon

Open Questions

Issues to Watch and Remaining Questions Prior to Act Roll Out

1. What requirements will be included in the standard contractual clauses?

2. What level of effort is expected to retrofit old systems to the Data Act?
   a) What is reasonable?
   b) Do compliance concerns trump reasonableness?

3. Can US companies make requests under the Data Act?

Compliance Approach

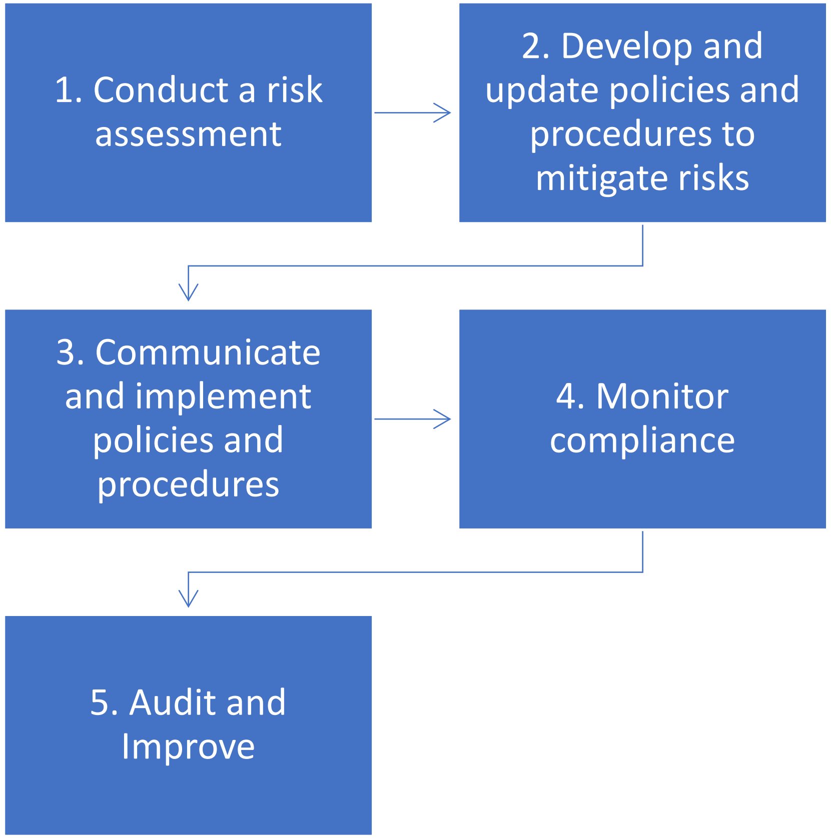
Lynn Parker Dupree
Naim Surgeon
Nicole Beranek Zanon

Privacy+ Security Forum

Stakeholder Education- Compliance Roadmap

1. **Bring in Stakeholders to Develop a Compliance Roadmap**
    a) The roadmap should identify:
        I. All data that is within the scope of the Act
        II. Practices that will be out of compliance following roll out
    b) Once the Roadmap is created, stakeholders should be educated about their roles and responsibilities and assigned tasks to address any technical work related to the Data Act
        I. These tasks should include:
            i. Review of pre-existing confidentiality and data sharing contracts
            ii. Data platform compliance updates
            iii. Business model optimization

Sample Compliance Roadmap



1. Conduct a risk assessment

2. Develop and update policies and procedures to mitigate risks

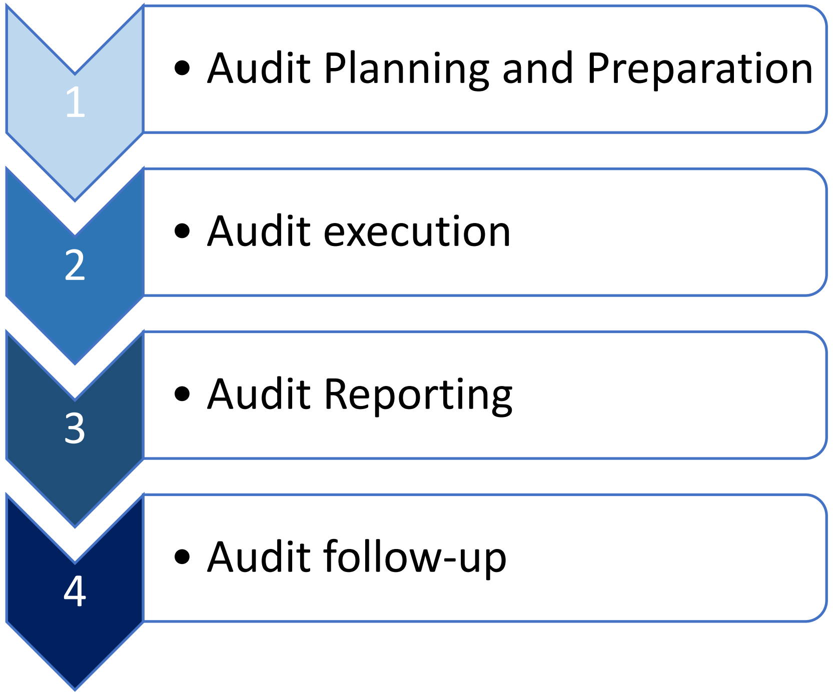
3. Communicate and implement policies and procedures

4. Monitor compliance

5. Audit and Improve

Stakeholder Education- Readiness Audit

2. Engage with Third-Party to Conduct a Readiness Audit
   a) Prior to an audit, stakeholders should:
      I. Align on and define the scope and depth of the audit
      II. Complete a pre-audit assessment
      III. Establish potential points of concern based on internal review
      IV. Engage in audit
      V. Prioritize action items based on audit findings



1
- Audit Planning and Preparation

2
- Audit execution

3
- Audit Reporting

4
- Audit follow-up

What You Need To Do

- Customize your product
- Inform customers about your connected products before they sign a contract!
- Define which data is covered by the data provision obligation?
- Conclude data license agreements with users of your connected products or connected services!
- Only disclose data to authorized parties!

Questions & Contacts

Lynn Parker Dupree
Partner
Finnegan, Henderson, Farabow, Garrett & Dunner LLP
lynn.parkerdupree@finnegan.com

Naim Surgeon
Managing Attorney
NextEra Energy Resources
naim.surgeon@nexteraenergy.com

Nicole Beranek Zanon
Lic. Iur., Exec.MBA HSG
HARTING Attorneys at Law Ltd.
Beranek@Haerting.ch