EU Data Act 2026: From Compliance Requirements to Implementation - Webinar Report

---

Executive Summary

The webinar **“EU Data Act 2026: From Compliance Requirements to Implementation”** focused on turning the EU Data Act into a practical implementation program. The presenters emphasized that readiness requires more than data export—it involves clear scoping, data inventories, access models, operational controls, updated contracts, and cross-functional governance.

Bas Overtoom and Mónica Fernández Peñalver explained how the Act enables users to access data generated by connected products and, where requested, share it with designated third parties. They highlighted the distinction between raw product data and processed or aggregated information.

A key focus was the **12 September 2026** milestone for data access by design in new connected products. The session covered direct and indirect access models, with direct access preferred where feasible and indirect processes serving as an alternative or fallback.

The Data Act in practical terms

Connected products, related services, and the data ecosystem

The deck defines a connected product as an item that obtains, generates, or collects data concerning its use or environment and can communicate product data through an electronic communications service, physical connection, or on-device access. Its primary function is not the storage, processing, or transmission of data on behalf of a party other than the user. A related service is a service connected to the product and essential to its functioning, excluding communications and software as described in the deck.

The presenters cautioned attendees not to limit their scope exercise to the physical product. Bas Overtoom noted that organizations may focus on the device yet overlook connected services, such as apps or insights services, that form part of the product ecosystem. The elevator example made this concrete: a connected elevator may generate sensor readings, camera footage, app data, and usage data that are valuable to the building owner and a maintenance company as well as to the elevator provider.

Actor	Webinar explanation	Operational implication
User	An owner of a connected product, a person with temporary contractual rights to use it, or a recipient of related services.	User journeys must support access to relevant product data.
Data holder	The party that retrieved or generated the data from a connected product and must make it available.	The organization needs accountable ownership for access, request handling, safeguards, and evidence.

Data recipient	A user or third party to whom the data holder makes data available.	Processes must support user-directed sharing and appropriate verification.
Public body	A body that may request data in specified exceptional circumstances.	Organizations need a route to receive, assess, and respond to such requests.

The wider regulatory picture

The deck grouped the Data Act into thematic pillars covering general provisions, data access and sharing, fair contracts, public-sector access, cloud switching and interoperability, international transfers, enforcement and safeguards, and final provisions. Bas Overtoom said that data sharing and contractual arrangements were the principal focus of this webinar, while public-sector access was also highlighted. Cloud switching and interoperability were noted as particularly relevant for cloud providers but were not explored in detail.

The presenters also emphasized that the Data Act should not be confused with the General Data Protection Regulation (GDPR). Bas described the Data Act as concerning product-data sharing, whereas GDPR concerns the protection of individuals' privacy. Mónica added that where generated product data is personal data, organizations must still comply with GDPR when sharing it with users or third parties and should reflect this interaction in both practice and contract terms.

Readiness milestones and the audience's starting point

The deck highlighted three timing messages. It states that users may request access to data generated during product operation since 12 September 2025. It identifies 12 September 2026 as the point by which new connected products must have data access designed in. It also identifies 12 January 2027 for the elimination of cloud/data-transfer switching charges and 12 September 2027 for specified older or indefinite-duration contracts.

Mónica explained that the new-product milestone does not require every access journey to be fully automatic. She described data access by design as allowing direct access where possible, with indirect access available as an alternative. The practical question for organizations is therefore not simply whether they have a portal or can send a file manually. It is whether their product and process design can deliver the relevant data in an appropriate, timely, and controlled way.

The webinar poll underscored the scale of the work still ahead for many participants. Bas summarized the response distribution as follows.

Poll stage reported by the presenter	Approximate share of respondents	Interpretation offered in the session
Had not started	30%	A substantial group had not yet begun Data Act activity.
Unsure what the Data Act is	10%	Combined with the “not started” group, approximately 40% required foundational awareness and scoping.
Assessing scope and obligations	Nearly 20%	Organizations were still in the first implementation stage.
Implementing	Around 20%	These respondents were updating contracts, processes, and/or technology.
Nearly complete, with gaps	Around 10%	Work remained to close residual compliance gaps.
Implemented and monitoring	Around 10%	A smaller group reported continuous-improvement activity.

These percentages are the presenters' rounded summary of the live webinar poll. They should not be treated as representative of the market as a whole.

Designing workable data access and sharing

Direct and indirect access

The webinar described two principal models. Direct access allows the user to download or stream generated data without involving the data holder. The presenters characterized this as the preferred approach where it is possible, while recognizing that it can be technically difficult, especially where data is processed inside a product and cannot be accessed without opening the product or redesigning the architecture.

Indirect access uses a request mechanism—such as an online form—backed by a process that validates the request, extracts the relevant data, provides access instructions, and delivers the data without undue delay. Mónica gave examples ranging from packaging and sending historic data to supporting real-time delivery through a suitable webhook. She stressed that the Data Act does not prescribe a general fixed response time for ordinary indirect access requests. Organizations should communicate a delivery timeframe and be able to show that their processes respond in a timely manner within what is technically feasible. Her reference to one month was presented as an example, not a universal statutory deadline.

Model	Webinar description	Design considerations raised in the session
Direct access	The user downloads or streams generated data without involving the data holder.	Product architecture, technical interfaces, availability, and data access built in from design.

Indirect access	The user requests data through a mechanism supported by validation and backend delivery processes.	Authentication, verification, access control, security, instruction design, request ownership, and delivery timing.
Hybrid approach	A direct mechanism can coexist with indirect access.	Indirect access can be a practical fallback for future product developments or new data that the direct mechanism does not yet cover.

Third-party sharing and public-body requests

A user may ask the data holder to send product data to a third party. The elevator scenario again provided the example: a building user may ask for data to be shared with a repair or maintenance company. The presenters said this will commonly be handled through an indirect route, with the data holder arranging instructions and any relevant contract or agreement needed to protect the data. If a third party is acting on the user's behalf, Mónica said the data holder should ask for a legal mandate as proof of that authority.

The deck and transcript also distinguish public-body requests. The presenters stated that, in the scenario described, an emergency request should receive a response within five days and a non-emergency request within 30 days. This is different from the less prescriptive ordinary access timing discussed for users and third parties.

Data quality, format, and timeliness

The deck says data should be made available in a comprehensive, structured, commonly used, machine-readable format and gives XML, JSON, and CSV as examples. It states that formats subject to licensing constraints are not "commonly used." Mónica added that the general rule of thumb is to give the user data in the same quality in which it is available to the data holder. The deck encourages real-time or continuous sharing where feasible, low-latency access for IoT scenarios, and automated workflows that reduce manual steps.

This means that an organization's data-access design should answer several questions at once: what data is covered; whether it is available directly or must be extracted; how a user is authenticated; whether personal, confidential, or trade-secret considerations need safeguards; in what format the data will be delivered; and how it will demonstrate timely handling.

What data is in scope: key clarification from the Q&A

The transcript materially clarified a question that was only visible as an attendee concern in the prior materials: whether a service provider may still use data to create insights and statistics, and whether users are entitled to raw, derived, or aggregated data.

Bas Overtoom answered that the Data Act, as discussed in the webinar, does not prevent a service provider from using data to create insights, statistics, or service improvements. He noted that other requirements may apply, including consent in some circumstances, but said this use is not stopped by the Data Act. Mónica Fernández Peñalver then clarified that the data to be shared is raw data generated by the product and metadata necessary to interpret that raw data where available. She gave sensor readings, such as temperature metrics, as examples. In contrast, processed, enriched, or aggregated statistics created after the fact were described as outside the sharing scope explained in the webinar.

Practical distinction from the discussion: *Product-generated raw data, plus necessary available metadata, should be identified during scoping. Derived reports, statistics, and enriched analytical outputs should be classified separately rather than assumed to follow the same access path.*

Contracts, terms, and safeguards

The presenters described contract terms as the second major implementation area after data-sharing solutions. The deck uses FRAND to mean "fair, responsible and non-discriminatory" terms and frames the purpose as protecting weaker parties, including by ensuring they receive the data-access rights they should have.

The contract checklist presented during the webinar included the data covered; access mechanics; user rights to use data and share it with third parties; restrictions on the data holder's use; confidentiality and trade secrets; security; the personal-data/GDPR interface; data quality and liability; compensation or pricing; duration and termination; product or service changes; audit, records, and evidence; and dispute resolution and remedies. 2

The Q&A provided a useful practical clarification on where these provisions can appear. In response to a question about whether the information must sit in an individual contract, Bas said organizations can use terms and conditions and policies to set out Data Act and data-delivery updates. However, appropriate contractual referencing or an agreement with users that terms and conditions can be updated may be required. He stressed that it is not necessary to have a separate individual contract with every user; the provisions can form part of the terms and conditions through which the contract is provided.

Mónica outlined several possible implementation paths: amend the contract, add a suitable appendix, revise terms and conditions, or add a set of additional terms, while communicating amendments to customers. She also noted that the Data Act leaves room for interpretation in some cases, making documented justification for the chosen contractual approach important.

Practical implementation lessons

The recurring challenge: governance across teams and entities

The webinar drew on examples from organizations developing environmental-monitoring devices, connected industrial equipment, and connected electric-vehicle charging equipment with digital energy-management services. Across these contexts, the presenters said the recurring challenge is coordination: deciding which entity owns the obligation, who validates users, who handles requests, who communicates changes to terms, and how responsibilities work across a complex organizational structure.

The recommended answer is not a generic policy alone. Mónica described designing processes that can then be reflected in policies suitable for group-level use or smaller subsidiaries. Those policies should be sufficiently flexible to

accommodate different product teams and future developments, while still making responsibility and decision routes clear.

A sequenced but parallel roadmap

The deck illustrated a 16-week implementation roadmap. It begins with a decision tree on applicability and requirements, followed by a data-in-scope inventory and data-sharing policy. It then addresses request and approval-flow design, divisional implementation, technical data sharing where needed, contract drafting or terms updates, and contract rollout.

Mónica said such a program can sometimes be faster or slower depending on organizational maturity. Bas summarized the work in three practical buckets: first, inventory and scope; second, technical implementation and process design; and third, contract readiness, which can be undertaken partly in parallel. He cautioned that the work cannot realistically be completed in a week, but neither does it have to take a year when an organization has a clear approach.

Workstream	Activities described	Intended result
Scope and inventory	Use product- and data-in-scope decision trees; record data points, decisions, and justifications.	A clear, supportable view of what falls in scope and what needs to be shared.
Data-access operating model	Select direct, indirect, or hybrid access; design request, validation, approval, delivery, instructions, and logging.	A functioning mechanism for users and appropriate third-party requests.
Technical controls and safeguards	Build access capability where applicable; address format, quality, timeliness, security,	A delivery approach that is usable and controlled.

	personal data, and trade secrets.	
Policy and contract alignment	Define roles, responsibilities, sharing conditions, and contractual or terms updates.	An operating model reflected in governance and commercial documentation.
Lifecycle governance	Reassess new products and new data sources as they are introduced.	A durable program rather than a one-time remediation exercise.

Why the data inventory must be maintained

Bas described the data inventory as a tool to identify the specific data points that may need to be shared and to remain current as new data enters the organization. The deck adds that the inventory should record scoping decisions and justifications, support assessment of future data sources, and identify trade secrets and personally identifiable information that require extra care.

This lifecycle approach is critical. A direct interface that works for current data may not cover a future product feature or a new type of data. The presenters therefore recommended retaining an indirect process as a safety net and embedding scope assessment into product development and procurement.

Audience Q&A: questions and answers that added practical guidance

The following Q&A synthesis is based on the recorded answers, edited for clarity while preserving the substance of the discussion.

Audience question	Webinar answer and practical significance
Can a service provider still use customer-generated data for aggregated statistics and product improvement?	Bas said yes: the Data Act does not prevent use of data to generate insights or improve services. He cautioned that consent and other requirements can arise under other regulations. The important implementation distinction is to identify these uses separately from the raw product data that must be made available.
Must a data holder share raw data, aggregated statistics, or both?	Mónica said the relevant data is raw product-generated data and necessary available metadata for interpretation. She said processed, enriched, or aggregated statistics fall outside the scope described in the webinar.
What does “new connected products” mean—existing products or newly created products?	Mónica explained that this refers to connected products placed on the market and put into service. The response highlights the need to assess placement and service context rather than relying only on a product’s development date.
Can Data Act requirements be communicated through terms and conditions or policies rather than an individual contract?	Bas said they can be addressed through terms and conditions and policies, provided the contractual arrangement appropriately references them or users have agreed to the update process. A separate contract for every user is not necessary.
Can a user request data later if the data holder has already deleted it?	Mónica distinguished Data Act product data from chat or other personal data. In the product-data scenario, if the data holder no longer has the data because it has been deleted, the user cannot access data that is unavailable to the holder. This makes data retention and availability

	an important part of the organization’s inventory and operating-model design.
Is a computer an IoT-connected device, and are app data included?	Mónica said a computer is a connected device, as is a phone, and used screen-time data as an example of data that can be made available. She distinguished standalone app-provider data: an app such as Instagram is not, in her example, a related service of the phone itself and therefore falls outside the Data Act context being discussed, although other regulations may apply.

Critical FAQ

1. What information must be shared under the approach described in the webinar?

The presenters said the relevant data is raw data generated by the connected product, together with metadata necessary to interpret it where that metadata is available. Examples included raw sensor measurements, such as temperature data, and location or device-identification information that helps a user understand which device produced the data. The discussion did not treat processed, enriched, or aggregated statistical outputs as data that must be shared under this access obligation.

2. May an organization still use product data to improve its services or create aggregated insights?

Yes, according to Bas Overtoom’s Q&A response. The Data Act does not stop a service provider from creating insights, statistics, or service improvements from data. However, he noted that other regulatory requirements, including consent in some circumstances, may be relevant. Organizations should not assume that Data Act analysis replaces privacy, contractual, or other compliance analysis.

3. What is the difference between direct and indirect data access?

Direct access enables the user to download or stream generated data without involving the data holder. Indirect access uses a request process and backend delivery workflow, supported by authentication, verification, security, access controls, and instructions. Direct access should be provided where possible, but an indirect route can be appropriate where direct access is not technically feasible and can operate as a fallback for new data types or future product changes.

4. Can a user ask for product data to be sent to a maintenance provider or another third party?

Yes. The webinar described the user's right to ask that data be sent to a third party, using an elevator maintenance company as an example. In practice, this will commonly be an indirect process. The data holder should establish the appropriate instructions, safeguards, and relevant agreements. When a third party is acting on the user's behalf, the webinar recommended requesting evidence of legal authority.

5. Is it necessary to add a separate Data Act contract for every user?

No. The Q&A stated that relevant requirements can be set out through terms and conditions or policies, rather than through an individual contract with every user. The organization should ensure that the terms are properly incorporated or referenced in the contractual relationship and that users have agreed to the relevant update process where necessary.

6. What happens if the requested product data was deleted before the user asks for it?

Mónica said that if the data holder no longer has access to the data because it has been deleted, the user cannot access it from that holder. This does not determine all data-retention requirements, but it makes it important to map data availability and retention practices when designing the Data Act operating model.

7. Do personal-data obligations disappear when an organization shares product data under the Data Act?

No. The presenters stressed that the Data Act and GDPR have different purposes. When generated product data is also personal data, organizations still need to navigate GDPR requirements when sharing with a user or third party and should address the interaction in their controls and contract terms.

8. How long does implementation normally take?

The presentation showed an illustrative 16-week implementation roadmap. Mónica said the duration can be faster or slower depending on organizational maturity, while Bas said it is a project that cannot realistically be completed in a week but should not need a year when the organization has a clear approach. Scope, product complexity, data architecture, existing controls, and contract footprint will affect the actual timeframe.

Key takeaways and next steps

The most important first action is to conduct a structured product, service, and data scope assessment. Organizations should identify connected products and related services; distinguish raw product-generated data from processed or aggregated outputs; record the metadata needed for interpretation; and document the reasons for inclusion or exclusion. The inventory should also flag personal data, trade secrets, and security-sensitive data.

Second, organizations should define the operating model for access and sharing. This involves choosing the appropriate direct, indirect, or hybrid mechanism; building authentication and authority verification; establishing procedures for user-directed third-party sharing; defining formats and delivery expectations; and making sure that the design has documented safeguards and owners. An indirect mechanism should not be treated as an improvised manual response; it is a controlled process with customer instructions, validation, and delivery steps.

Third, organizations should address contracts and terms in parallel with operational design. Contractual documents and policies should accurately reflect the data covered, access mechanics, user and third-party rights, confidentiality, security, data quality, liability, and the interface with GDPR. Where terms and conditions are used, they need to be appropriately incorporated into the contractual relationship.

Finally, leaders should establish ongoing governance. Scope decisions and data inventories must be revisited as products evolve, new data is collected, and new related services are introduced. The webinar’s practical lesson is that Data Act

compliance is not a one-off legal review; it is a maintained capability across product development, technology, commercial practices, and governance.