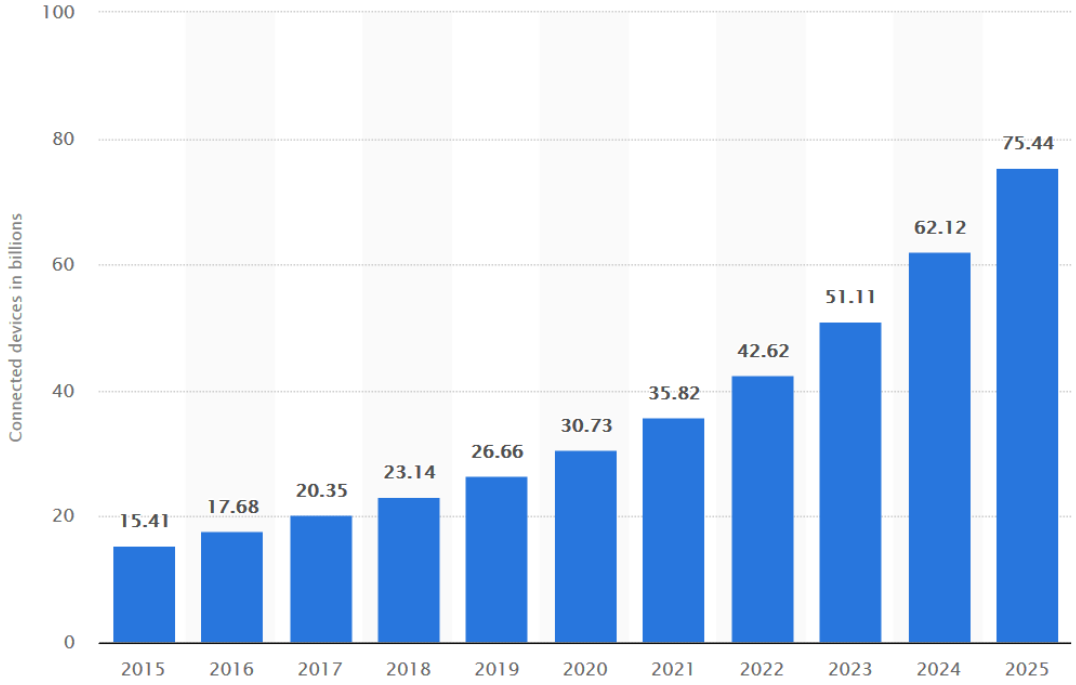
GDPR compliance for IoT: from design to deployment

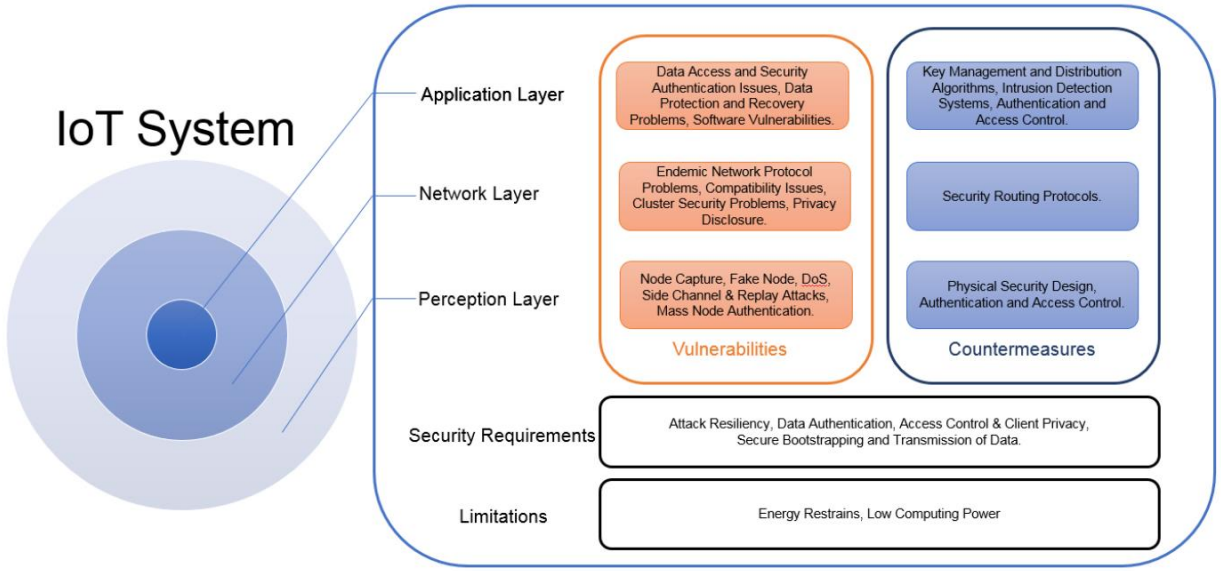
Adrian Quesada Rodriguez
MSc. MA. CIPP/E
Researcher on Law and ICT
Mandat International

MANDAT INTERNATIONAL

Fundamentals:

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



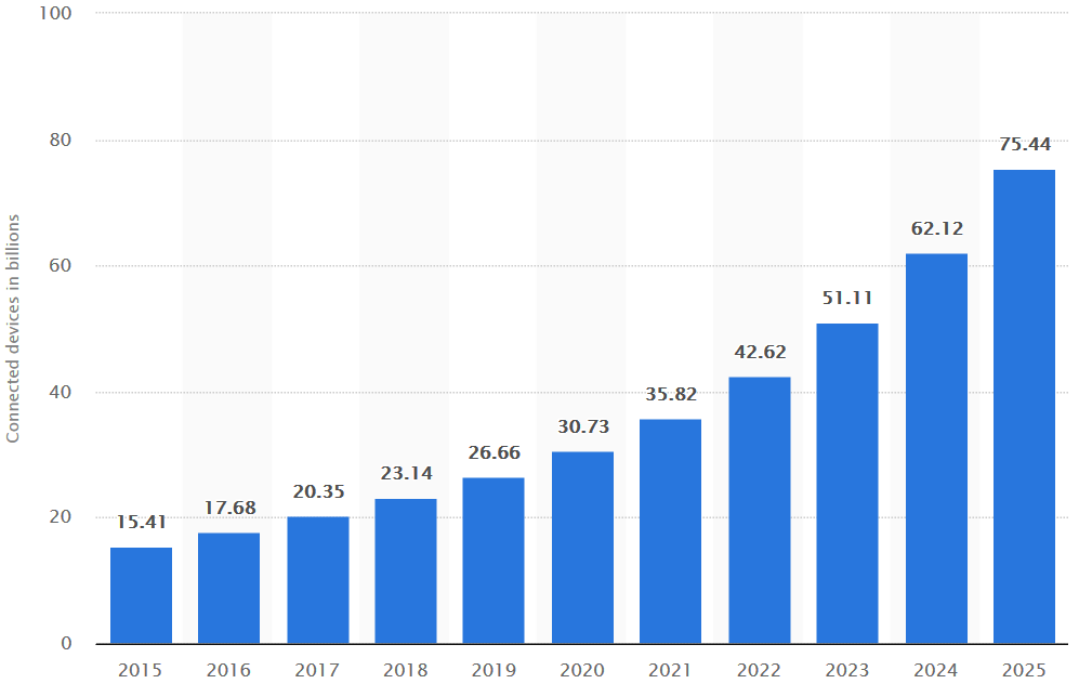


Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ and "Internet of Things: Survey on Security and Privacy" by Diego M. Mendez, Ioannis Papapanagiotou, Baijian Yang (Purdue University) https://arxiv.org/abs/1707.01879

MANDAT INTERNATIONAL

Fundamentals:

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



VS

GDPR principles (art. 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitations
- Integrity and confidentiality

Approach: Personal data protection and security by design and default (art. 25)

Requirements:

- Organizational: Consent and proof of consent, Underage consent, DPIA…
- Technical: Encryption, anonymization, access management…
- Administrative: Data breach reports to DPA

Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

MANDAT INTERNATIONAL

Privacy by design?

- Concept originally postulated by Ann Cavoukian, based on 7 foundational principles:

1) Proactive not Reactive, Preventative not Remedial
2) Privacy as the Default: no opt-in required!
3) Privacy embedded into Design: privacy enhancing (not reducing) functionality!
4) Full functionality – Positive sum, not Zero-Sum: no need for privacy/security tradeoff!
5) End-to-End Security: Lifecycle protection of information.
6) Visibility and Transparency: trust but verify!
7) Respect for user privacy: keep it user-centric!

See: Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Implementation?

IoT must adopt the personal data protection and security by design and by default approach

Devices and associated software:

- Minimize personal data
- Hide PD and metadata
- Separate: distributed processing and storage
- Aggregate
- Inform
- Control
- Enforce privacy policy
- Demonstrate

IoT deployments:

- Human-centric
- Isolated
- Transparent roles
- Single point of contact
- Non-discriminatory
- Independent privacy and security audits
- Dynamic trust KPIs and metrics
- Continuous monitoring

Coordination is required throughout BOTH information and supply chains!

See Hoepman, J. H. (2014). Privacy design strategies. ICT Systems Security and Privacy Protection, 446–459 and EC Report on workshop on Security and Privacy in IoT
http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf

MANDAT INTERNATIONAL

IoT chain and privacy roles

- Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

- Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

- Joint controllers (Rec. 79; Art. 4(7), 26): Where two or more Controllers act together they are “Joint Controllers” and must, by means of an “arrangement” between them, apportion data protection compliance responsibilities.
  - (Rec. 79, 146; Art. 26(3), 82(3) - (5) – Joint Controllers are jointly and separately liable

MANDAT INTERNATIONAL

IoT chain and privacy roles, how to address them?

- Contractual dispositions

Appointment of Processors (Rec. 81; Art.28(1)-(3))

A Controller must only appoint a Processor under a binding written agreement, which states that the Processor must:

(i) only act on the Controller's documented instructions; –
(ii) impose confidentiality obligations on all personnel who process the relevant data;
(iii) ensure the security of the personal data that it processes; –
(iv) abide by the rules regarding appointment of sub - processors;
(v) implement measures to assist the Controller in complying with the rights of data subjects; –
(vi) assist the Controller is obtaining approval from DPAs where required; –
(vii) at the Controller's election either return or destroy the personal data at the end of the relationship; and –
(viii) provide the Controller with all information necessary to demonstrate compliance with the GDPR

- European data protection board: what is relevant is how things work in practice

See ENISA report on Privacy and Data Protection by Design – from policy to engineering https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design and Art. 29 WP opinion on the concept of "controller" and "processor" https://www.hldataprotection.com/uploads/file/wp169_en.pdf

MANDAT INTERNATIONAL

IoT chain and privacy roles, how to address them?

- Appointment of a DPO!
- Direct coordination with all interested parties
- Interventability-enhancing techniques
- Certification mechanisms
- Strong audit/verification activities
- Real time privacy and security controls
- DPO decision support and organizational compliance tools

See ENISA report on Privacy and Data Protection by Design – from policy to engineering https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design and Art. 29 opinion on DPOs http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

MANDAT INTERNATIONAL

GDPR certification

Certification mechanisms (Recital 76, 81 and Art. 42)

- Data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.
- Data protection certification mechanisms, seals or marks (…) may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation (…) within the framework of personal data transfers to third countries or international organisations.
- The certification shall be voluntary and available via a process that is transparent.
- A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation

- Products and services / Information management systems
- GDPR / Swiss and international obligations
- Integrated approach with relevant ISO standards (including ISO/IEC 27001)
- Designed to address emerging technologies

See ENISA recommendations on European Data Protection Certification

MANDAT INTERNATIONAL

Technical and organizational compliance tools

Keep track of personal data flows throughout the organization or enterprise

- Real time, network level privacy and security threat/vulnerability monitoring
- Dynamic Security and Privacy Seal
- Decision support for DPO/Sysadmin
- Audit logs / Certification surveillance solutions

MANDAT INTERNATIONAL

Some final thoughts

- DPOs cannot do it all by themselves: Personal Data Protection must involve all levels of management and constant education for end-users and employees alike.

- Security-wise, the GDPR does not introduce any requirements that shouldn't already be in place in a responsible organization. However, in the context of IoT, it does require innovative (and thoughtful) approaches to be introduced, especially if end-users are concerned. Consider data usage and understand your own system!

- A chain is only as strong as the weakest of it’s links: Technology vendors and software providers can be both your downfall and your salvation.
  - Cloud services / services based outside of EU should also be considered!

- Traditional compliance is not enough: personal data protection should go beyond the implementation of security controls to address the expected risks, adaptive compliance is necessary!

MANDAT INTERNATIONAL

Thank you!

Questions?

aquesada@mandint.org