MAI4CAREU

Master programmes in Artificial
Intelligence 4 Careers in Europe

University of Cyprus

MAI650 Internet of Things

Vasos Vassiliou

September - December 2023

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CS6xx Internet of Things (8 ECTS)

Course purpose and objectives: The purpose of the course is to provide an overview on IoT tools and applications and to introduce to students hands-on IoT communication concepts through lab exercises.

Learning outcomes: Upon completion of this course, students will be able to explain the definition and usage of the term “Internet of Things” in different contexts. More specifically, the students will know how to apply the knowledge and skills acquired during the course to build and test a complete, working IoT system involving prototyping, programming and data analysis

Teaching methodology: interactive face-to-face lectures, group activities and discussions, in class/lab activities, student presentations and guest lectures or significant recorded public lectures

Assessment: Final exam (50%), midterm exam (20%) and assignments/project (30%).

Main text:

Rajkumar Buyya, Amir Vahid Dastjerdi, Internet of Things Principles and Paradigms, Morgan Kaufmann; 1st edition, 2016

J. Biron and J. Follett, "Foundational Elements of an IoT Solution", O'Reilly Media, 2016.

Other reading:

Jamil Y. Khan and Mehmet R. Yuce, Internet of Things (IoT) Systems and Applications, 2019, ISBN 9789814800297

David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2016, Cisco Press.

INTRODUCTION

Security and Privacy in IoT - Core

CONTENTS

1. Introduction
2. Consumer Guidelines
3. Security by Design
4. The Code of Practice - Guidelines

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

INTENDED LEARNING OUTCOMES

Upon completion of this introductory unit, students will be:

1. familiar with the the term security by design
2. familiar with the security principles
3. familiar with the software development life cycle
4. familiar with the code of practice guidelines.

Introduction

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Security by Design

- IoT Security system
  - All stakeholders should follow security principles and guidelines to protect the users
- IoT stakeholders
  - IoT vendors and manufactures
  - IoT Service Provides
  - IoT Software Developers
  - IoT Consumers
  - Policymakers and government agencies

- Security guidelines
  - IoT Consumer
  - IoT Software Developer
  - IoT manufactures
  - IoT service provides

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Security by Principles

- Authentication
  - Authenticate devices and users to prevent malicious access
- Encryption
  - Encrypt data to prevent access to it and eavesdropping
- Security in all areas
  - Devices, apps, service providers
  - Perform regular vulnerability tests
- Updates
  - Provide updates securely with minimal impact
- Privacy
  - Disclose privacy related policies such as data collection but keep the collection to the minimum required
- Disclosures
  - Have disclosures that cover privacy policies, data collection and functionality
- Control
  - Consumers should have the choice to control on the data collected
- Communication
  - Use best practices communication techniques with the device owners to limit social engineering attacks

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Consumer Guidelines

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Prominent Threats

- Distributed Denial of Service Attack (DDoS)
  - Botnet network with zombie machines
  - The attacker chooses a victim and sends a signal to all the zombies to launch the attack.

- Mirai
  - Turns network devices running Linux O/S into remotely controlled bots.
  - Targets: consumer devices such as IP cameras and home routers
  - IoT devices that the consumers did not change their factory default usernames and passwords
  - Reboot device to remove the malware and change password

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Hosting the Enemy

- Mrs. Soulful got a Christmas present from her children
  - A system for making her kitchen “smart”
  - Keep postponing the update
  - The smart system became unbearably slow

- Hospital patient record system did not respond
  - Cloud services
  - DDoS

[2] ENISA. "Towards secure convergence of Cloud and IoT," September 17, 2018.

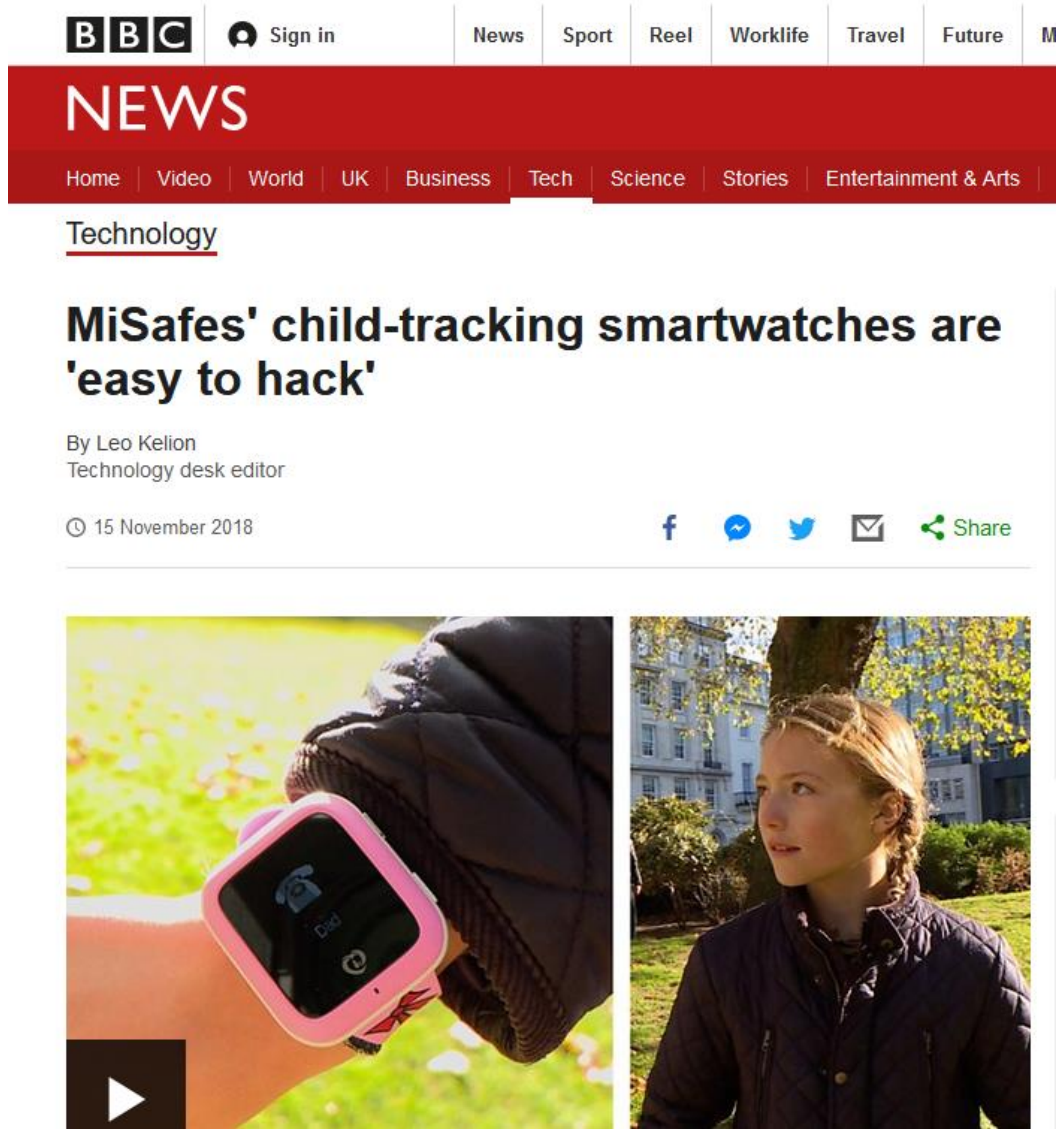
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Consumer Guidelines

- DDoS

- Invasion of privacy
  - Wearables



Technology

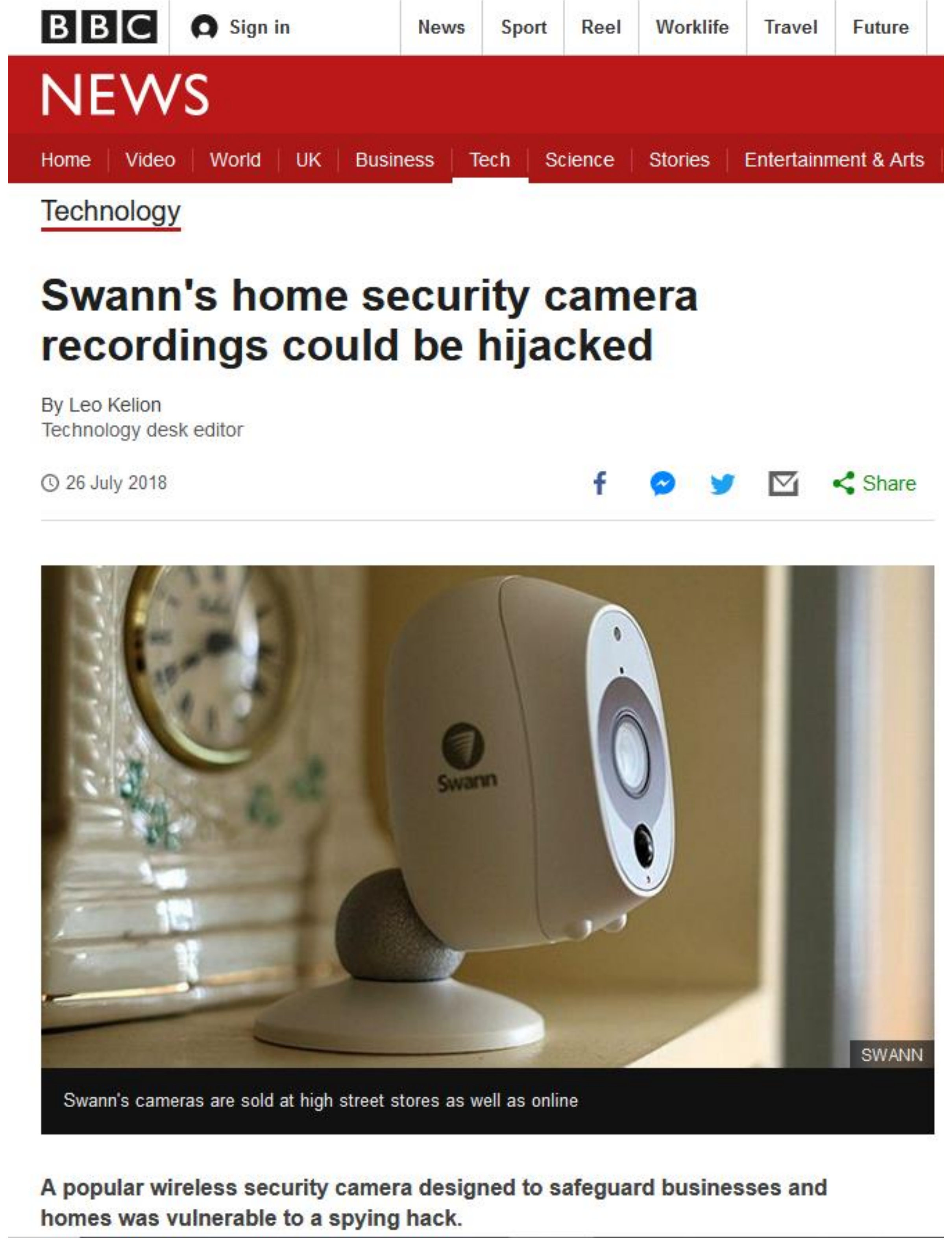
MiSafes' child-tracking smartwatches are 'easy to hack'

By Leo Kelion
Technology desk editor

15 November 2018

Consumer Guidelines

- DDoS
- Invasion of privacy
  - Wearables
  - Home Cameras



Technology

Swann's home security camera recordings could be hijacked

By Leo Kelion
Technology desk editor

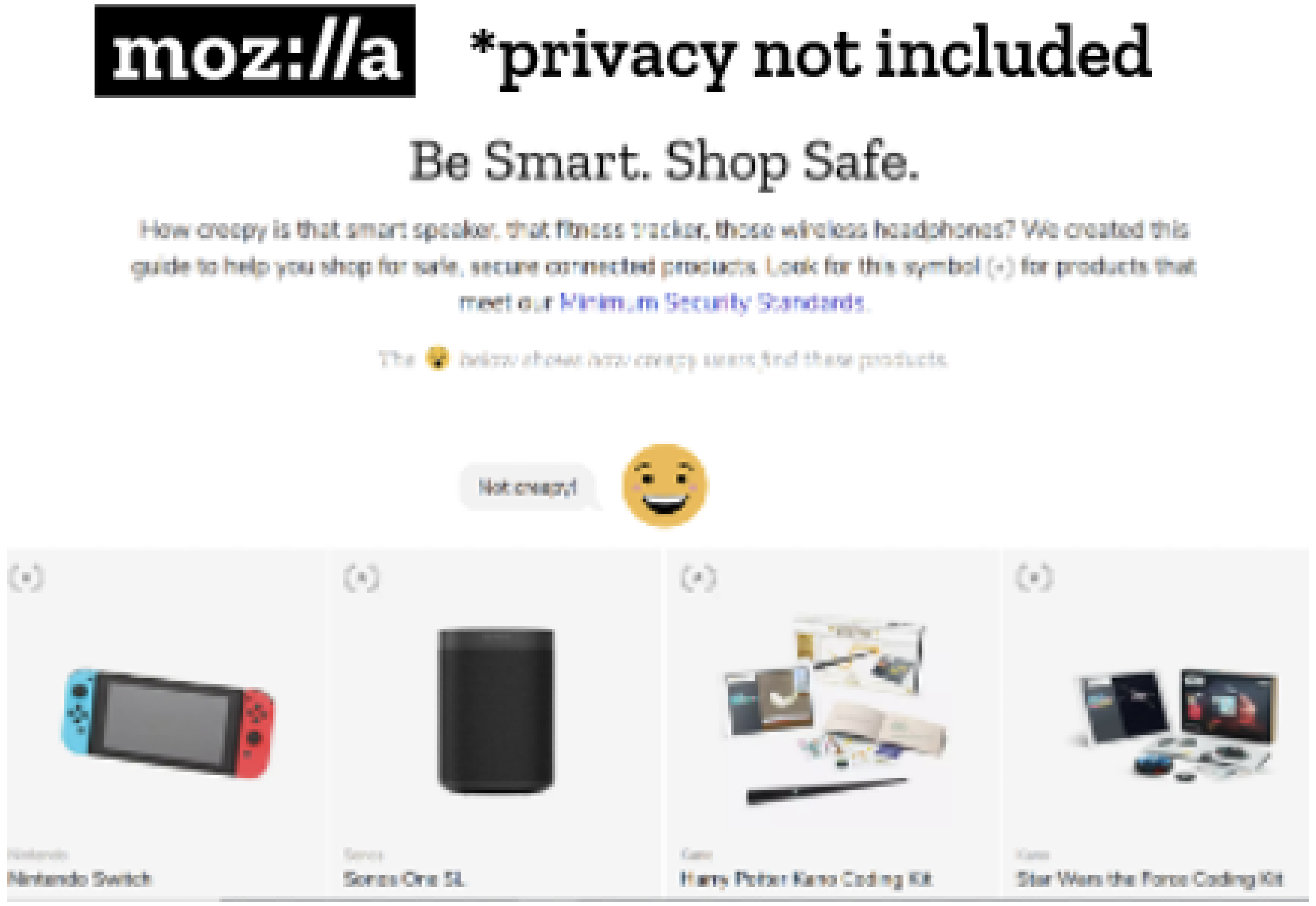
26 July 2018

Swann's cameras are sold at high street stores as well as online

A popular wireless security camera designed to safeguard businesses and homes was vulnerable to a spying hack.

Consumer Guidelines

- Setting up your device
  - Before you buy, check reviews of the product and the manufacturer



moz://a *privacy not included

Be Smart. Shop Safe.

How creepy is that smart speaker, that fitness tracker, those wireless headphones? We created this guide to help you shop for safe, secure connected products. Look for this symbol (•) for products that meet our Minimum Security Standards.

The 😮 below shows how creepy users find these products.

https://foundation.mozilla.org/en/privacynotincluded/
*Accessed January 2010

[3] Department for Digital, Culture, Media and Sport, UK . “Smart devices: using them safely in your home," October 14, 2018.

Consumer Guidelines

- Check the default settings
  - Some devices may be insecure when they are first switched on.

  - Changed the password
    - Secure password – not guessable
    - Do not reuse password

Consumer Guidelines

- Managing your account
  - Default passwords
  - Two factor Authentication (2FA)
    - Are you who you are claiming to be?
    - Two security checks
    - Use it on your email accounts too

Consumer Guidelines

- Keeping your device updated
  - Switch on the option to enable automatic updates
  - Install any manual updates when prompted
  - Make sure your device’s operating system is up to date

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Consumer Guidelines

- If something goes wrong
  - If for any reason you think that your device is affected, then visit the manufacturer’s website
    - https://www.samsung.com/global/galaxy/security/
    - https://www.apple.com/uk/privacy/control/
    - https://safety.google/security/security-tips/
    - https://support.microsoft.com/en-ae/help/4013263/windows-10-stay-protected-with-windows-security
    - ..
  - Visit your country’s cyber security centre
  - Someone has malicious control/access of a device
    - Perform factory reset.

Consumer Guidelines

- Getting rid of your device
  - **Factory reset!**

Consumer Guidelines - The 6 Basic Guidelines

1. Setting up your device
2. Check the default settings
3. Managing your account
4. Keeping your device updated
5. If something goes wrong
6. Getting rid of your device

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Security by Desing

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Introduction

- Software
  - The Application
  - Network Protocols

- Mrs. Soulful smart system
  - Updates
  - DDoS

Security by Design

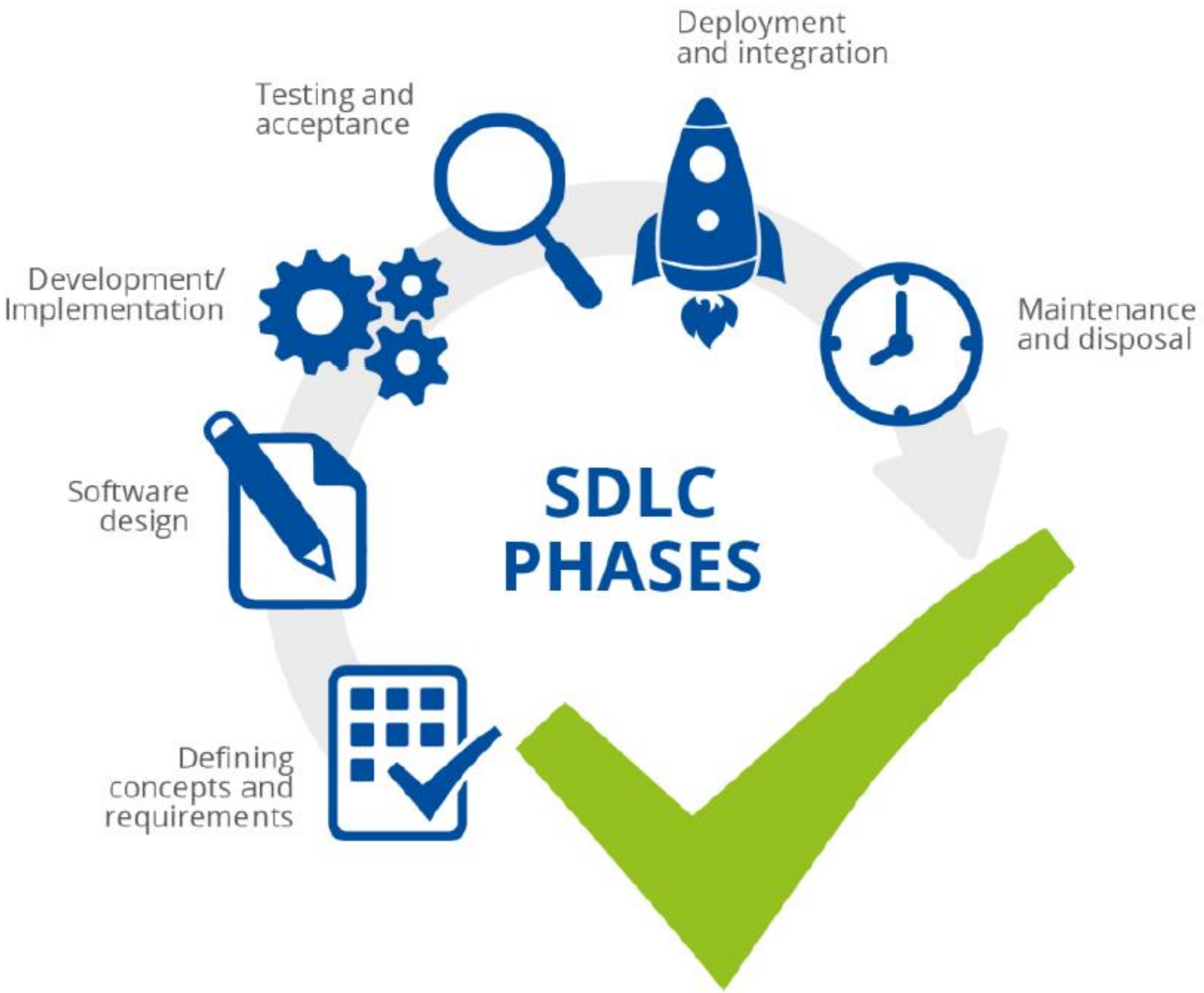
- Software
  - IoT Apps
  - Software Development Kits (SDKs)
  - IoT platforms
  - Application Programming Interfaces (API)
  - Operating Systems
  - Development of communication protocols

- Security by design
  - IoT Software Development Life Cycle (SDLC)

- Software Development Life Cycle – SDLC
  - A process consisting of different phases that aims at delivering and effective and efficient systems as per their design and functional requirements.
  - Multiple SDLC models
  - Consider Security across all phases

[1] ENISA, “Good Practices for Security of IoT: Secure Software Development Lifecycle," November 17, 2019.

Software Development Life Cycle


Deployment and integration
Testing and acceptance
Development/ Implementation
Maintenance and disposal
Software design
SDLC PHASES
Defining concepts and requirements

Software Development Life Cycle

Requirements

- Foundation of the software to be developed
- Security Requirements on the context and software functionality
  - Indicative security requirements
  - Software Functionality
- Hardware requirements
  - Root-of-Trust (RoT) mechanism
  - Hardware Security Module (HSM)
- Threat model
  - STRIDE - Spoofing, Tampering, Information Disclosure, Repudiation, Denial of Service and Elevation of Privilege

- Risk Analysis
  - Predefined checklists of most common security risks and pitfalls
  - OWASP IoT Top10
    1. Weak, Guessable, or Hardcoded Passwords
    2. Insecure Network Services
    3. Insecure Ecosystem Interfaces
    4. Lack of Secure Update Mechanism
    5. Use of Insecure or Outdated Components
    6. Insufficient Privacy Protection
    7. Insecure Transfer and Storage
    8. Lack of Device Management
    9. Insecure Default Settings
    10. Lack of Physical hardening

Software Development Life Cycle

Software Design

- Software Architecture and the IoT solution are created
- Threat model detail analysis including the probabilities of such attacks occurring
- Chain of Trust
- Recovery Plans
- Integration of security Mechanisms (remote credential management etc.)
- Enforcement of CIA triad, access control, policy configurations, and security lifecycles.

Software Development Life Cycle

Development/Implementation

- Implementing the software requirements and software design specification
- Secure code is the foundation of the IoT system
- Practice Secure Development (SANS Top 25 Software Errors)
- Secure code guidelines and coding standards
- Security assessment throughout the development phase
- Third party software

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Software Development Life Cycle

Testing and Acceptance

- Verification that the product follows all the requirements, design principles, security requirements defined in the previous phases
- Testing the software
  - Manual
  - Automated
- Design Review
- Security tests
  - Security Requirements Test
  - Static Analysis Security Testing (SAST)
  - Dynamic Analysis Security Testing (DAST)
  - Manual Code Review
  - Fuzzing test
  - Penetration tests

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Software Development Life Cycle

Deployment and Integration

- Integrate all IoT elements
- Deployment needs to carefully planned
- Hardware hardening
  - User-rights administration interfaces
  - Device authentications
  - User authentication
  - Self-enrolment requests
- Configuration and Vulnerability management
  - Review error messages send
- Change management

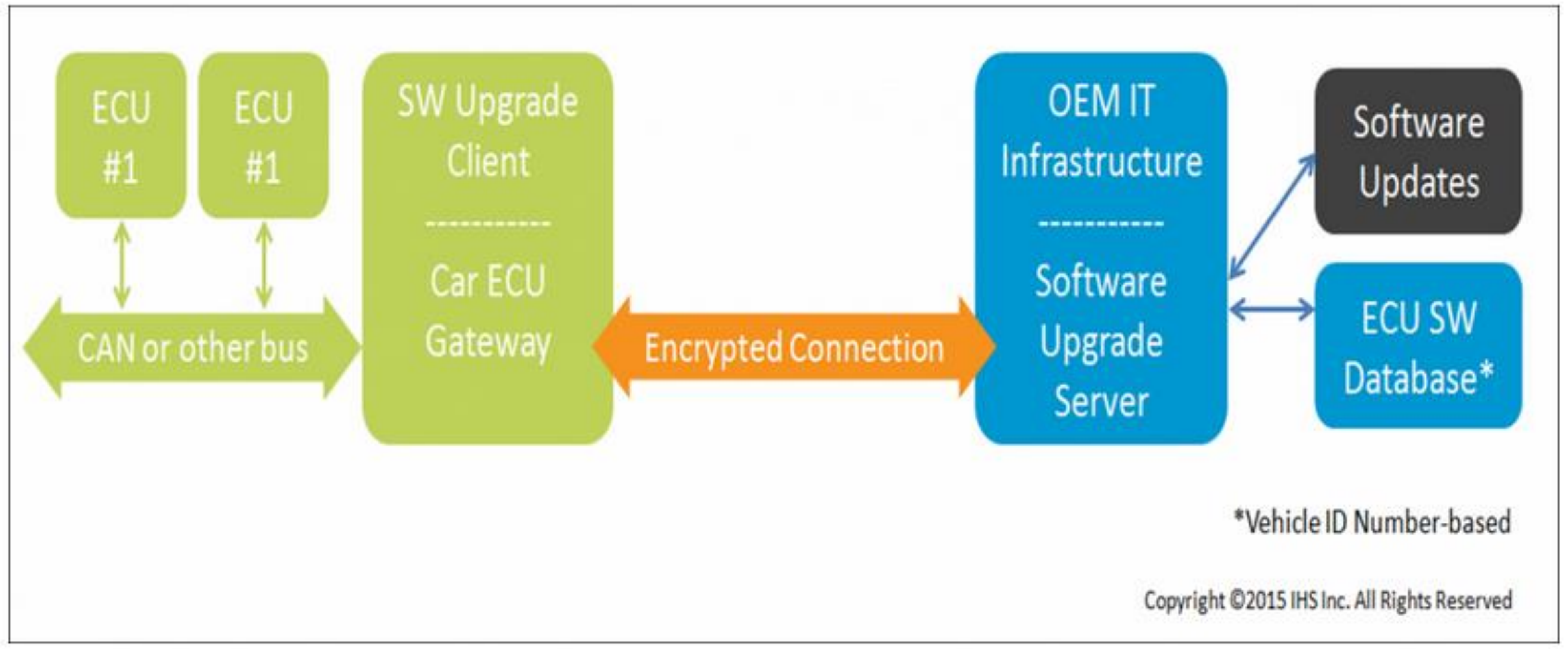
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Software Development Life Cycle

Maintenance and Disposal

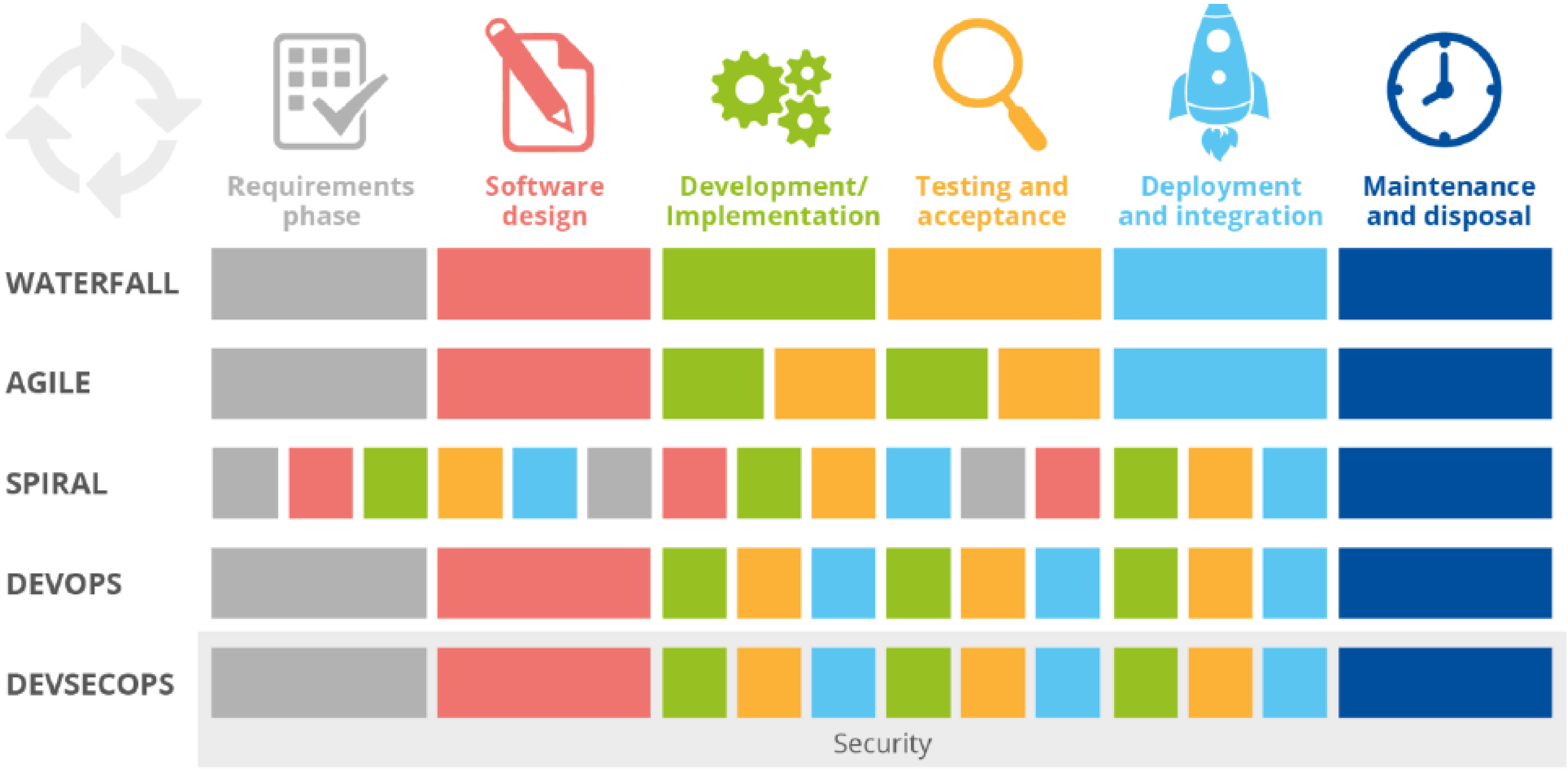
- Incident management
  - An ongoing process
  - Monitoring and Testing the system
- Remote software updates
  - or Firmware/Software Over the Air (FOTA/SOTA)
- Management of the disposal
  - Erase personal data
  - Erase credentials



*Vehicle ID Number-based

Copyright ©2015 IHS Inc. All Rights Reserved

Software Development Life Cycle



The Code of Practice

Guidelines

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

The Code of Practice - Guidelines

- Guidelines to ensure security by design
- Practical steps that focused on the outcome of the product
- Each guideline refers to different stakeholders
- The guidelines are prioritized based on their impact on security risks

The Code of Practice - Guidelines

Specific Group of Stakeholders

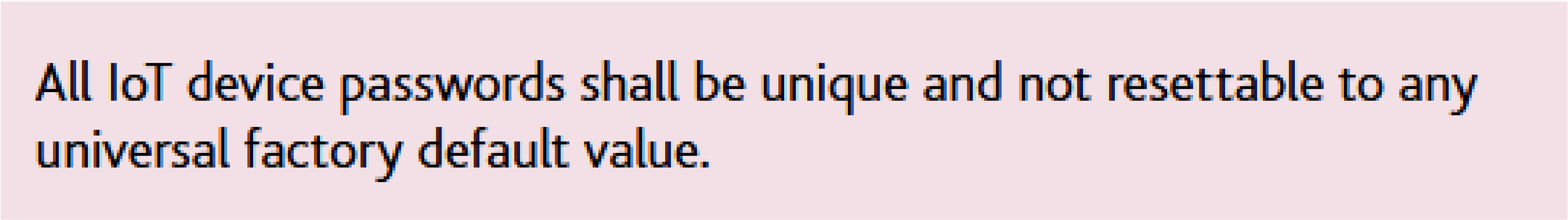
- Device Manufacturer
  - Final product that may incorporate third party products
- IoT Service Providers
  - Network service providers
- Mobile Application Developers
  - Software application development entities
- Retailers
  - The sellers of IoT elements including services

The Code of Practice - Guidelines

Guideline 1

- **No Default passwords**
  - Unique passwords
  - Avoid universal default usernames and passwords

- Applies to:
  - Device Manufacturers



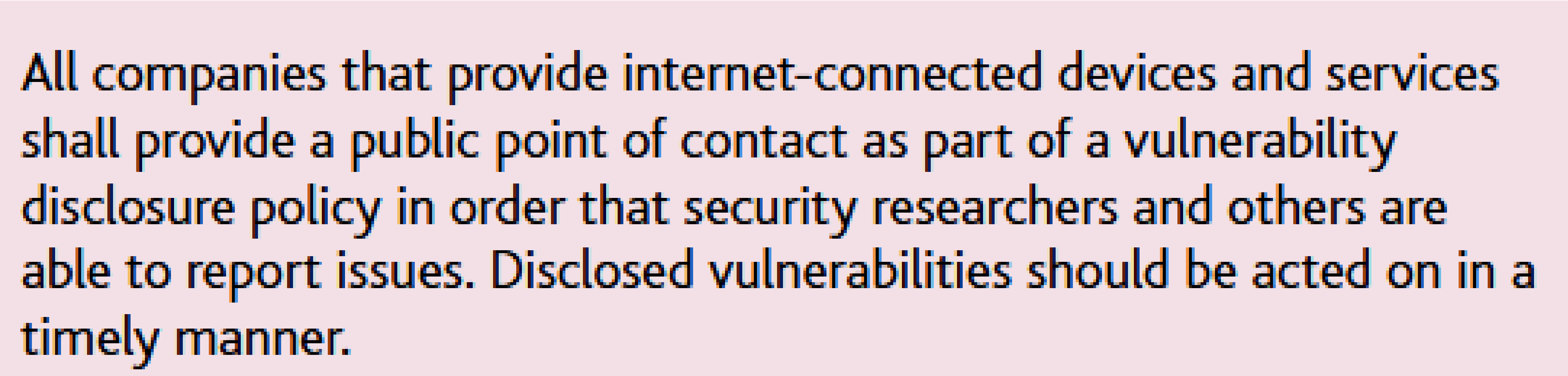
All IoT device passwords shall be unique and not resettable to any universal factory default value.

The Code of Practice - Guidelines

Guideline 2

- **Implement a vulnerability disclosure policy**
  - Inform of a security vulnerability
  - Monitoring the services and product for possible vulnerabilities

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers

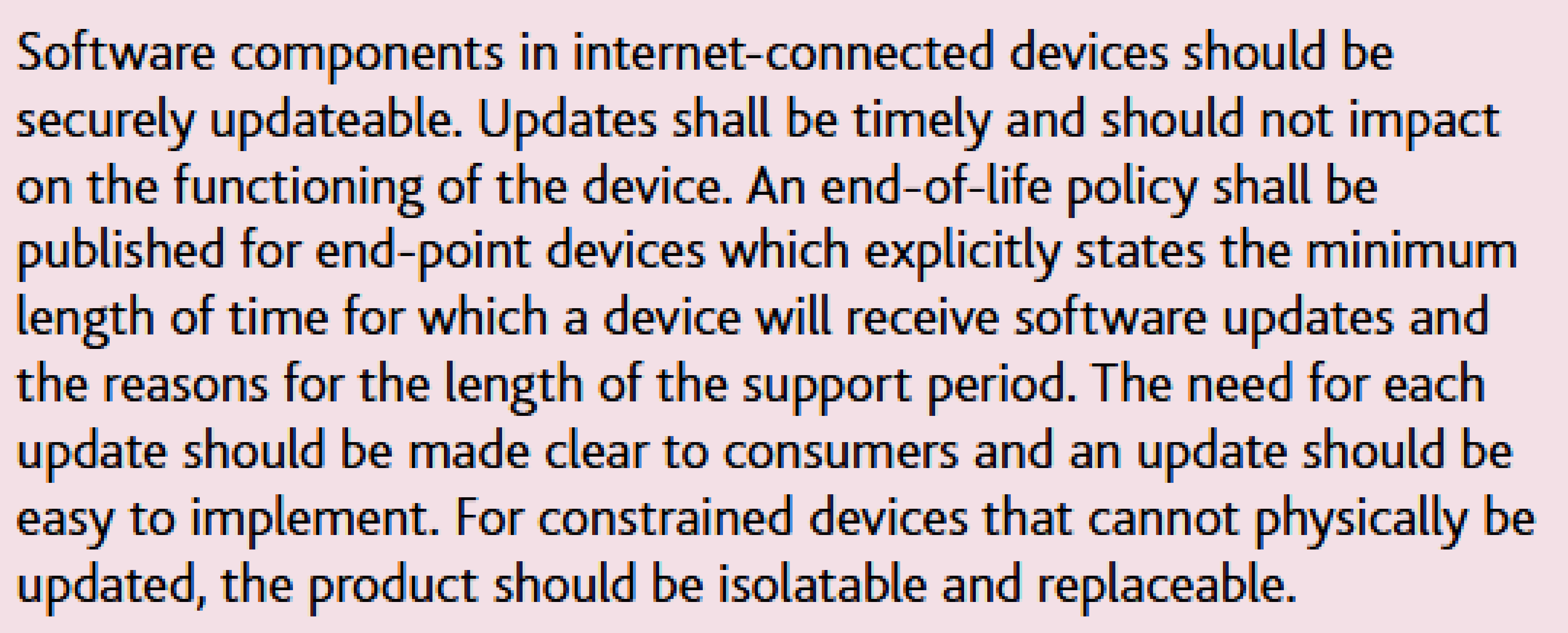


All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

The Code of Practice - Guidelines

Guideline 3

- **Keep software updated**
  - Updates for all purchased devices
  - Secure Channel when transmitted over the air
  - Maintain device functionality
- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



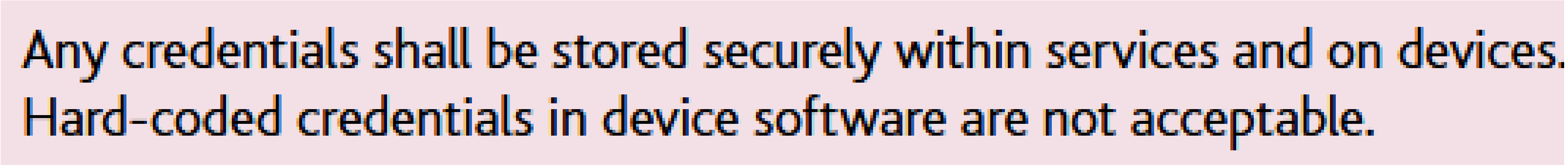
Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

The Code of Practice - Guidelines

Guideline 4

- **Securely store credentials and security-sensitive data**
  - Do not hard code the credentials

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.

Co-financed by the European Union
Connecting Europe Facility

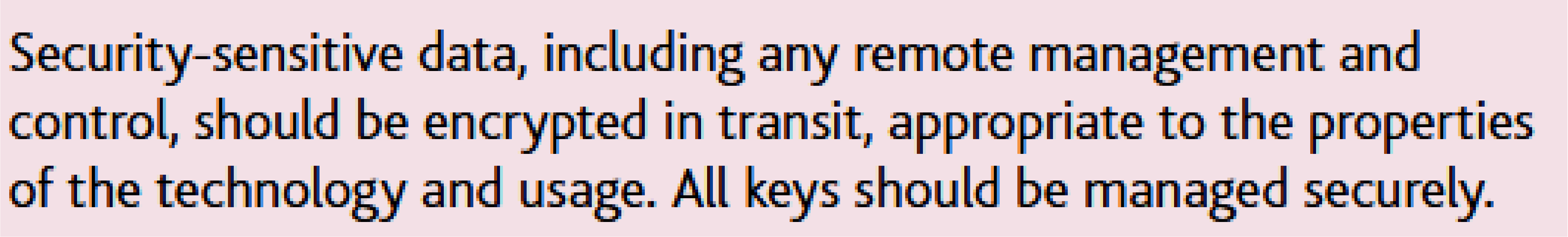
This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

The Code of Practice - Guidelines

Guideline 5

- **Communicate securely**
  - Use peer-reviewed standards

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



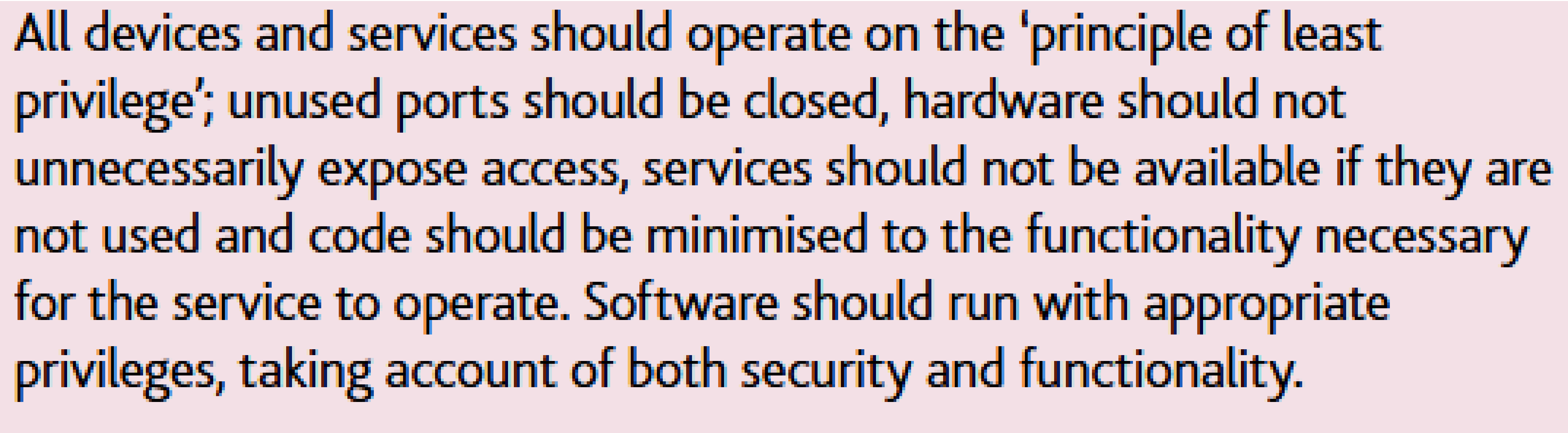
Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.

The Code of Practice - Guidelines

Guideline 6

- **Minimize exposed attack surfaces**

- Applies to:
  - Device Manufacturers
  - Mobile Application Developers



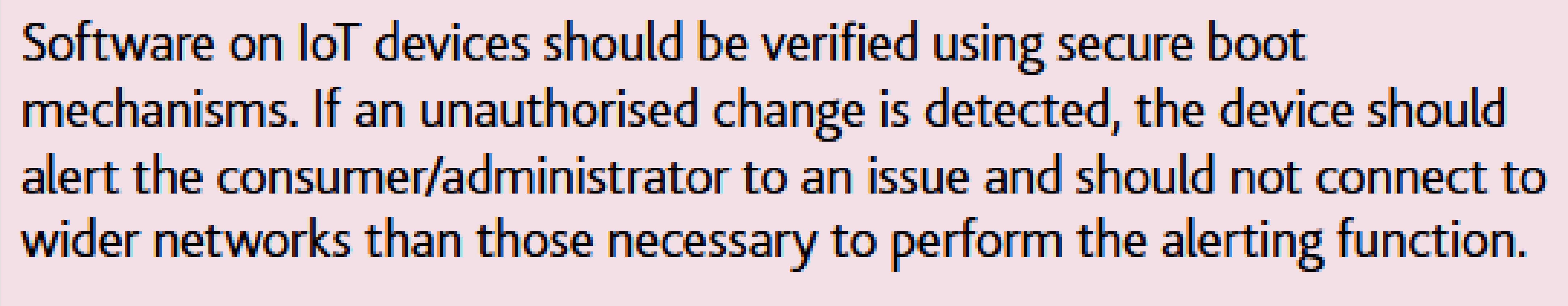
All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

The Code of Practice - Guidelines

Guideline 7

- **Ensure software integrity**
  - Remotely recover

- Applies to:
  - Device Manufacturers

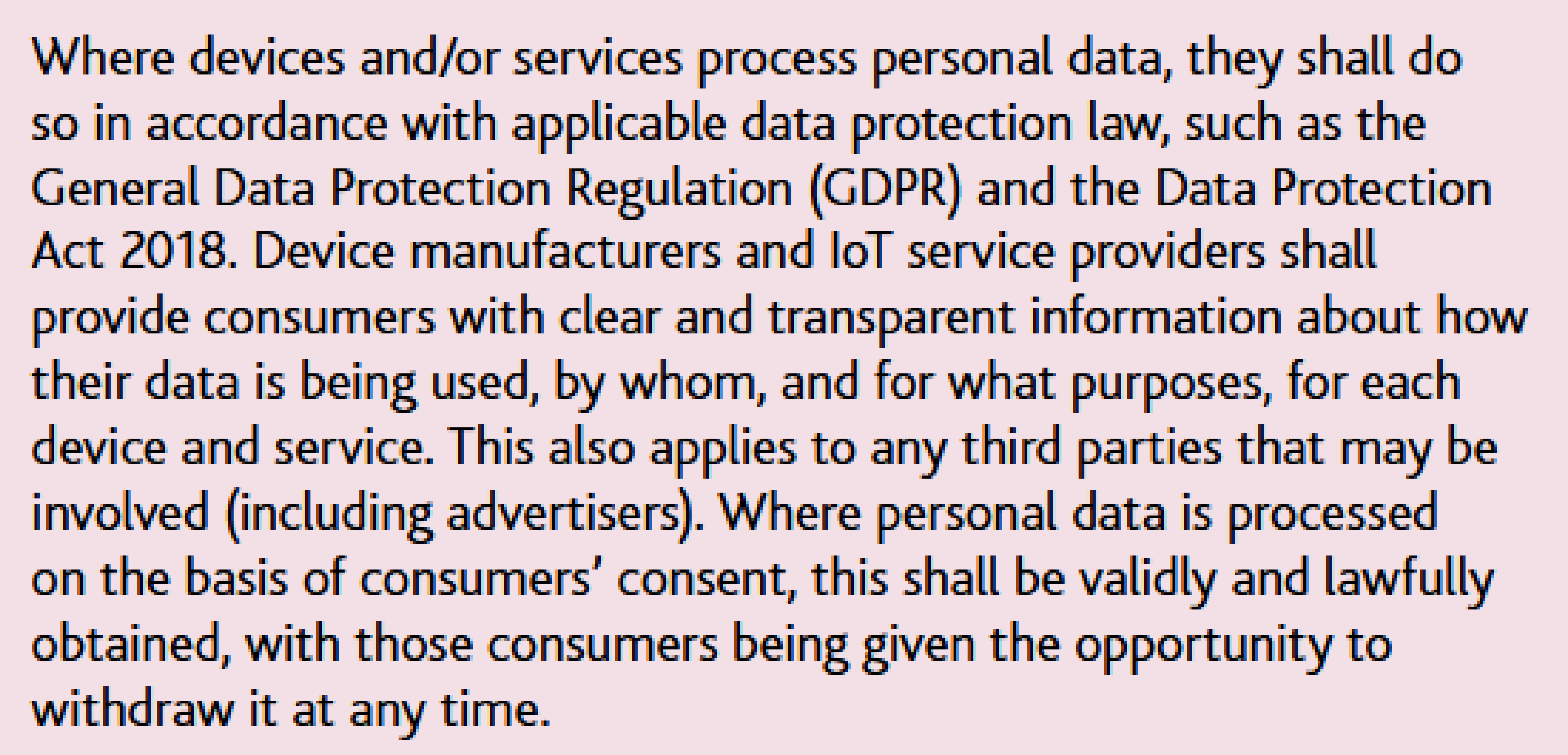


Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

The Code of Practice - Guidelines

Guideline 8

- **Ensure that personal data is protected**



Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

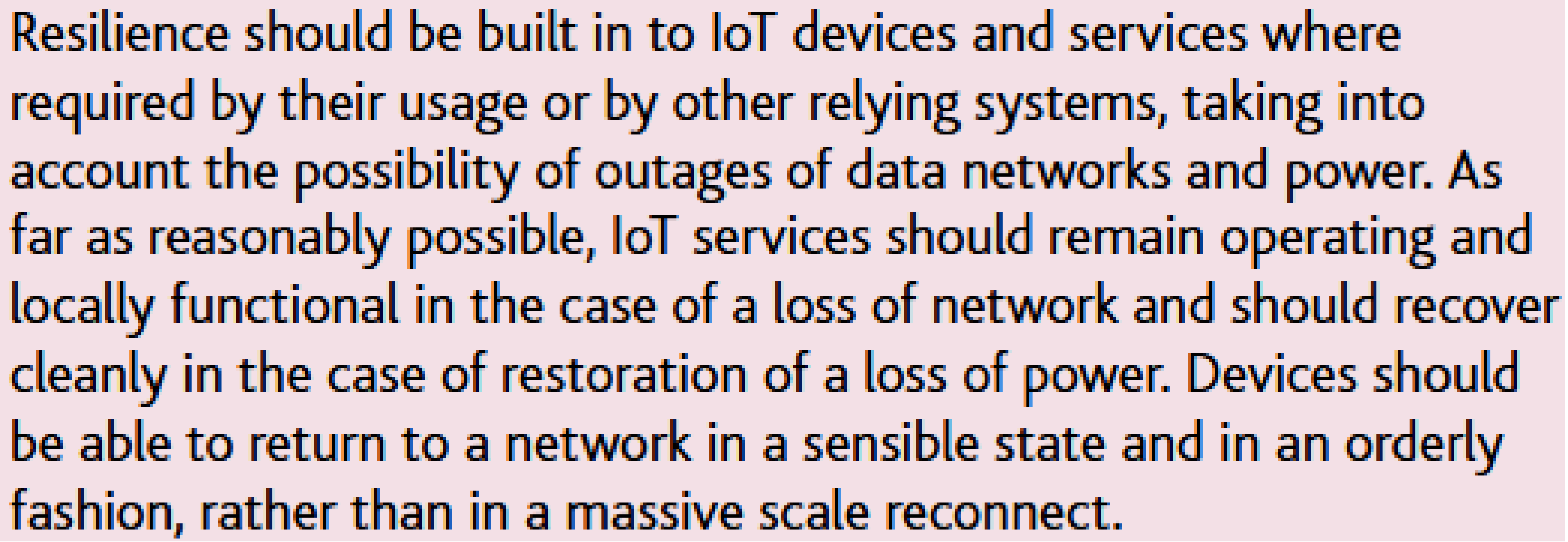
- Applies to:
  - IoT Service Providers
  - Mobile Application Developers
  - Retailers

The Code of Practice - Guidelines

Guideline 9

- **Make systems resilient to outages**

- Applies to:
  - Device Manufacturers
  - IoT Service Providers



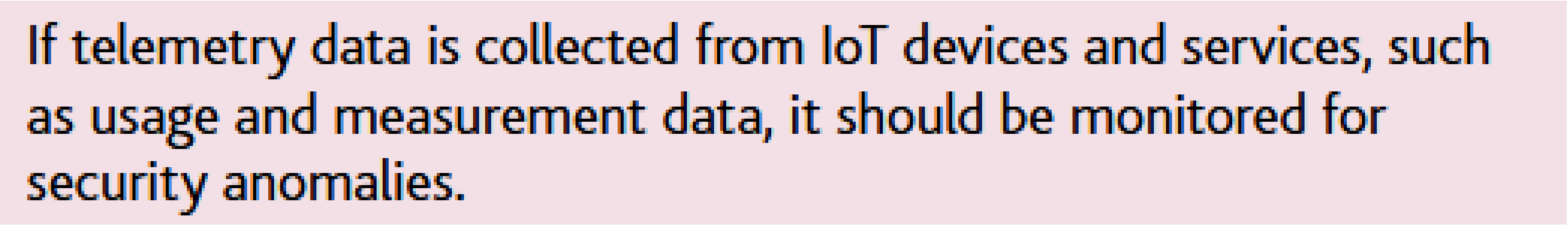
Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.

The Code of Practice - Guidelines

Guideline 10

- **Monitor system telemetry data**
  - Discover anomalies that can be used to the presence of an attack

- Applies to:
  - IoT Service Providers



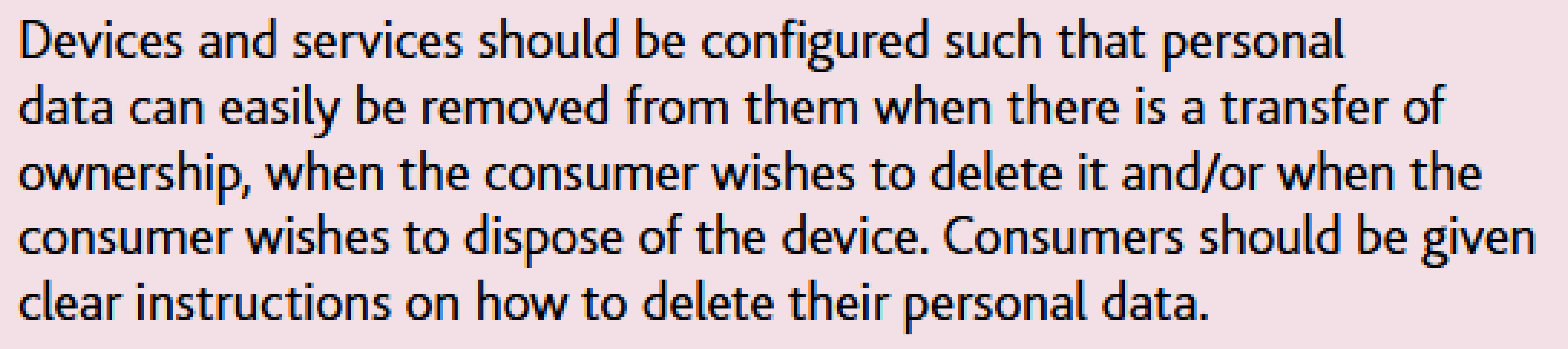
If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

The Code of Practice - Guidelines

Guideline 11

- **Make it easy for consumers to delete personal data**

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



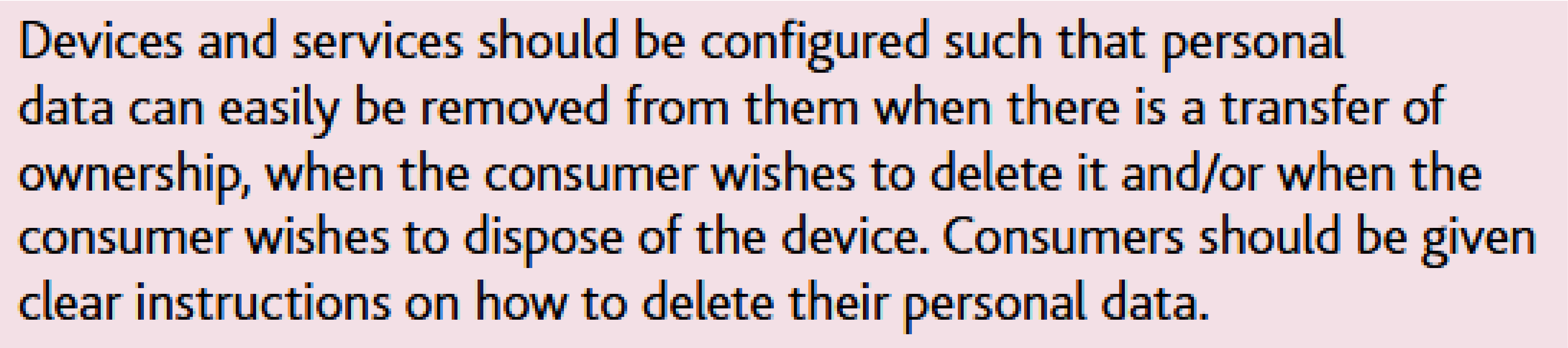
Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

The Code of Practice - Guidelines

Guideline 12

- **Make installation and maintenance of devices easy**

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



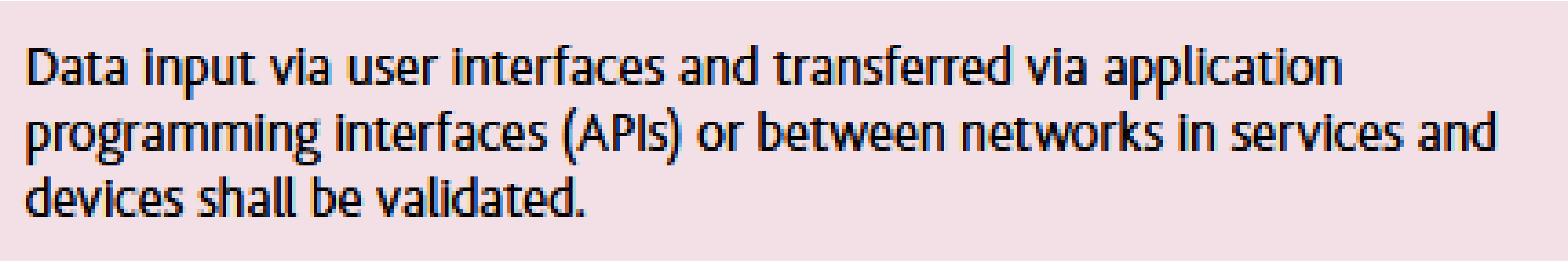
Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

The Code of Practice - Guidelines

Guideline 13

- **Validate input data**

- Applies to:
  - Device Manufacturers
  - IoT Service Providers
  - Mobile Application Developers



Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

The Code of Practice - Guidelines

Conclusion

- 13 Guidelines for integrating Security by Design
- The IoT applications are still expanding
- **Knowledge is power!**

Summary

- □ Introduction
- □ Consumer Guidelines
- □ Security by Design
- □ The Code of Practice - Guidelines

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423