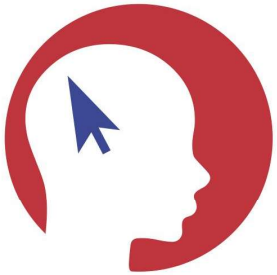


PRIVACYMINDERS

www.privacyminders.com | Email: info@privacyminders.com
Address: 57 Spyrou Kyprianou, Bybloserve Business Center,
6051-Larnaca, Cyprus | Tel: +357 24812581 Fax: +357 24812583

Οι δραστηριότητες των Ομάδων Εργασίας WG5 και WG8 της Ευρωπαϊκής Τεχνικής Επιτροπής CEN/CLC/JTC13 (Κυβερνοασφάλεια και Ιδιωτικότητα)

13| 12 | 2021

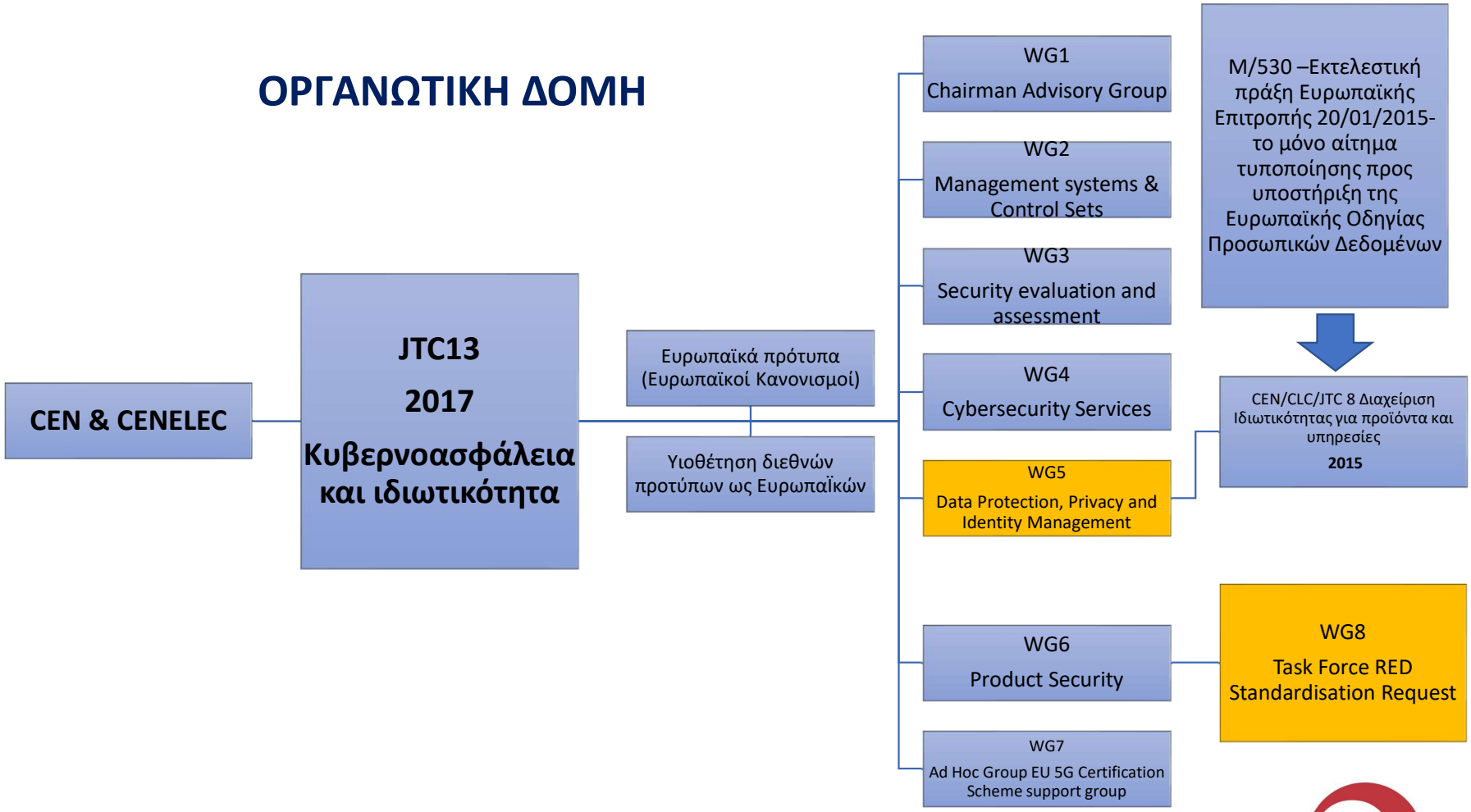
Maria Raphael

Lawyer, Privacy & Standardization Expert

CYS Delegate in CEN/CLC/JTC13

PRIVACYMINDERS

ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ



PRIVACYMINDERS

CEN/CLC/JTC13 WG5: Data Protection, Privacy and Identity Management

1. WG5 Consultations Task Force (Maria Raphael Convenor)
2. prEN 17926 Privacy Information Management System per ISO/IEC 27701-Refinements in European Context
3. FprEN 17529 Data Protection and privacy by design and by default (Revision)-Maria Raphael Acting Editor
4. prEN 17799 Personal Data Protection requirements for processing activities
5. prEN 17740 "Requirements for professional profiles related to personal data processing and protection"
6. FprCEN/CLC/TR 17919 Video Surveillance (TR-1 JT 013026)
7. Feasibility Study on "Certification Scheme as per ISO/IEC 17065 for Certification against ISO/IEC 27701 and NWIP Scheme for certification of PII processing operations
8. Adoption of ISO/IEC/SC27/WG5 Standards

→ AHWG ON Certification Schemes

CEN/CLC/JTC13/WG5/Consultations Task Force

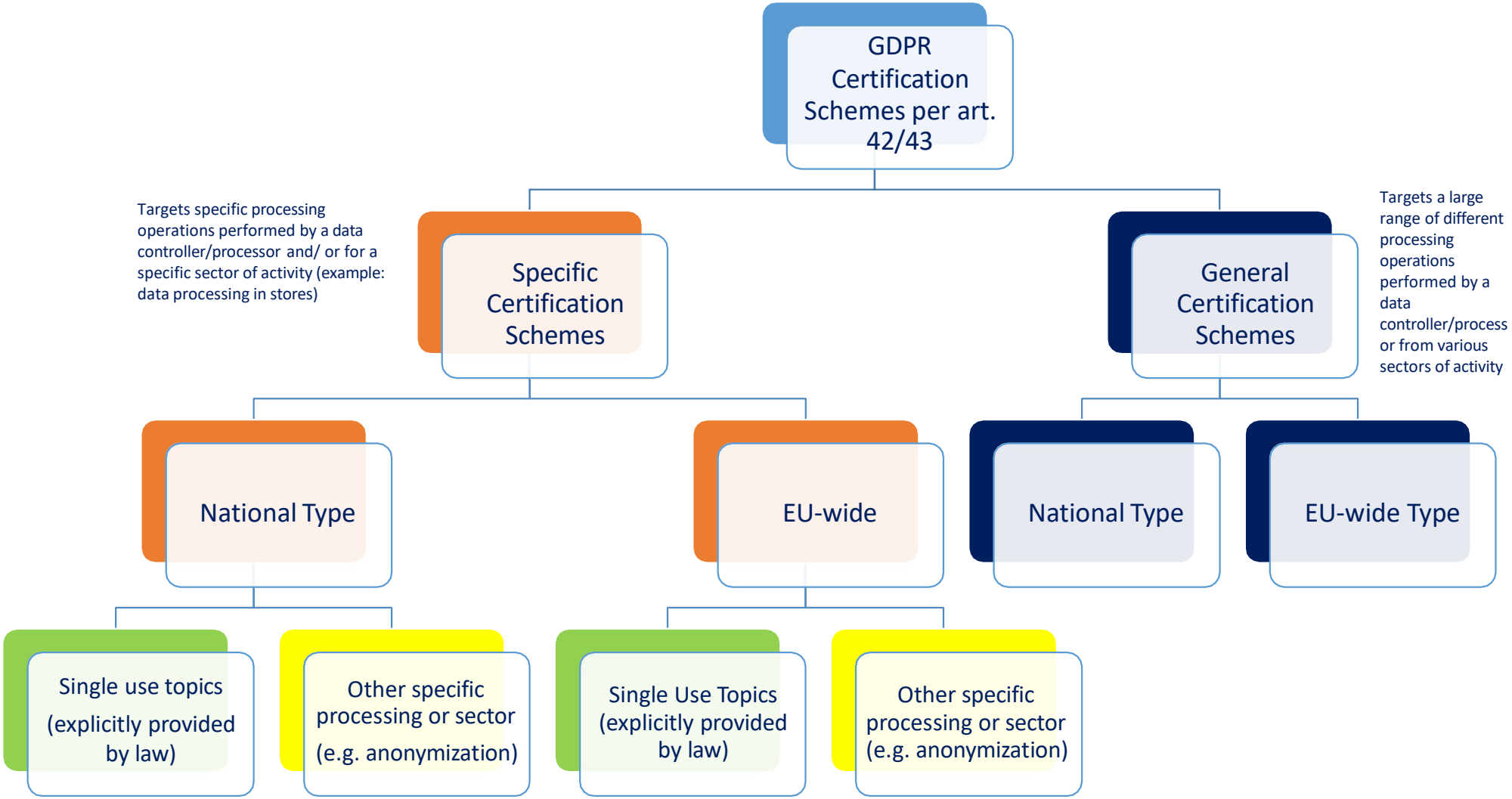
ΜΕΛΛΟΝΤΙΚΕΣ ΣΥΜΜΕΤΟΧΕΣ ΣΕ ΔΗΜΟΣΙΕΣ ΔΙΑΒΟΥΛΕΥΣΕΙΣ

- CYBER RESILIENCE ACT PROPOSAL

- Εγγραφή στην εικονική κοινότητα ενδιαφερομένων μερών για παροχή ανατροφοδότησης στο eIDAS Expert Group

Έργο 2022

- Ανατροφοδότηση επί των EDPB Guidelines 04 /2022 ‘’Calculation on fines under the GDPR’’
- Ανατροφοδότηση επί των EDPB Guidelines 07/2022 on Certification as tool for transfers


GDPR Certification Schemes per art. 42/43
Targets specific processing operations performed by a data controller/processor and/ or for a specific sector of activity (example: data processing in stores)
Specific Certification Schemes
General Certification Schemes
Targets a large range of different processing operations performed by a data controller/process or from various sectors of activity
National Type
EU-wide
National Type
EU-wide Type
Single use topics (explicitly provided by law)
Other specific processing or sector (e.g. anonymization)
Single Use Topics (explicitly provided by law)
Other specific processing or sector (e.g. anonymization)

GDPR CERTIFICATION AND STANDARDS (2022 and 2023 KEY FOCUS)

CEN/CLC/JTC13/WG5

JTO13037 "Privacy Information Management System per EN/ISO/IEC 27001-Refinements in European Context

JT01033 Personal Data Protection Requirements for processing operations (EN ISO/IEC 17067)

EN 17429 Data Protection & Privacy By Design and by Default

New Working items to assess DP certification Schemes against JT013037 and JT01033

Has the power to issue SR or promote technical standards for DP certification criteria as harmonised standards by way of implementing acts

Τα πρότυπα της WG5 που υποστηρίζουν την πιστοποίηση GDPR

Personal Data Protection Requirements for Processing Activities

- Specified baseline requirements for demonstrating compliance of processing activities with the EU Personal Data Protection Normative Framework in accordance with ISO/IEC 17065
- **It does not apply to products or management services but only to processing operations**
- It applied to all organisations, data controllers and processors
- It provides indications for third party conformity assessment (annex a)
- May support certification bodies, the supervisory authorities and the EDPB to develop GDPR Certification Schemes

NWIP Privacy Information Management System per ISO/IEC 27701-Refinements in European Context

- Application of ISO/IEC 27701 in European Context
- Specifies refinements to EN ISO/IEC 27701, **for processing operations as part of products, processes and services**
- **Aimed to management systems**
- CBs and SAs may use this standard to specify data protection certification mechanisms as per. Art. 42 GDPR
- CB can use these requirements and refinements to assess the conformity of both a privacy management system per ISO/IEC 17065 and the processing operations of a product, process or service per ISO/IEC 17065.

Data Protection & Privacy by design and by default" (EN17529) which provides guidance for compliance with art. 25 of GDPR and may be used to build a specific scheme. (M/530/2015)

PRIVACYMINDERS

Ο ρόλος της Ευρωπαϊκής Επιτροπής

Προώθηση μηχανισμών πιστοποίησης, σφραγίδων, σημάτων και προτύπων για να διασφαλιστεί η ομαλή και ομοιογενής εφαρμογή των προνοιών του ΓΚΠΔ

Κατ' εξουσιοδότηση πράξεις (43.8 ΓΚΠΔ)

Θέσπιση ενός γενικού πλαισίου που εξειδικεύει κριτήρια και απαιτήσεις για μηχανισμούς πιστοποίησης προσωπικών δεδομένων που δεν εξειδικεύονται στον ΓΚΠΔ για να τεθούν σε λειτουργία από κριτήρια που εγκρίνονται από DPA/EDPB

Εκτελεστικές πράξεις (43.9 ΓΚΠΔ)

Θέσπιση τεχνικών προτύπων για μηχανισμούς πιστοποίησης, σφραγίδων προστασίας δεδομένων και σημάτων και μηχανισμών για την προώθησή τους

PRIVACYMINDERS

Εκτελεστικές πράξεις (Τεχνικά πρότυπα)

Πρότυπα που καλύπτουν διαδικαστικά ζητήματα π.χ. ISO/IEC 17065 related to conformity assessment

Υποψήφια:

ISO/IEC Πρότυπα 17000 series e.g. ISO/IEC 17011: 2017 (conformity assessment-requirements for accreditation bodies accrediting conformity assessment bodies)

Εκτελεστικές πράξεις για προώθηση υπαρχόντων και μελλόντων τεχνικών προτύπων (που εκπονούνται με ή χωρίς αίτημα τυποποίησης) ως πρότυπα εναρμόνισης (43.9 GDPR)

Πρότυπα που αποτελούν τη βάση για να περιγράψουν τα κριτήρια πιστοποίησης έναντι των οποίων which compliance with the GDPR will be demonstrated

*EC Study on Data Protection Certification mechanisms (02/2019) does not recommend taking implementing acts to support implementation of available standards

PRIVACYMINDERS

CEN/CLC JTC 13/WG 5 Πρότυπα

Οι ιδιοκτήτες σχημάτων μπορούν να τα χρησιμοποιήσουν ως βάση για να αναπτύξουν τα δικά τους σχήματα πιστοποίησης

Η Ευρωπαϊκή Επιτροπής δύναται να τα προωθήσει ή άλλα Ευρωπαϊκά ή Διεθνή πρότυπα σχετικά με την πιστοποίηση GPDR ως εναρμονισμένα πρότυπα με εκτελεστικές πράξεις, αν συνάδουν με τις κανονιστικές ή διαδικαστικές πρόνοιες του ΓΚΠΔ

EDPB Guidelines 01/2018 on certification and identifying certification criteria in accordance with Art. 42 and 43 of the GDPR (Version 3.0)- 04.06.2019

- Η διαλειτουργικότητα κριτηρίων πιστοποίησης με άλλα πρότυπα (such as ISO ή εθνικά) διευκολύνει την έγκρισή τους
- Ενώ τα βιομηχανικά πρότυπα συχνά εστιάζουν στην προστασία και ασφάλεια του οργανισμού εναντίον απειλών, ο ΓΚΠΔ προσανατολίζεται στην προστασία ουσιωδών δικαιωμάτων φυσικών προσώπων. Η διαφορετική προσέγγιση πρέπει να λαμβάνεται υπόψη όταν σχεδιάζονται κριτήρια ή τυγχάνουν έγκρισης κριτήρια με βάση βιομηχανικά πρότυπα

PRIVACYMINDERS

CEN/CLC/JTC13/WG8 Special WG RED SR

Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2022/30 της Επιτροπής (29/10/2021)
→ Αίτημα τυποποίησης προς CEN and CLC

- Ενεργοποιεί τα άρθρα 3.3. (δ), (ε) και (στ) της Οδηγίας 2014/53/ΕΕ για τη διαθεσιμότητα ραδιοεξοπλισμού στην αγορά, τα οποία περιλαμβάνουν ουσιώδεις απαιτήσεις προς τις οποίες πρέπει να συμμορφώνονται οικονομικοί φορείς, εξειδικεύοντας τις κατηγορίες ή κλάσεις ραδιοεξοπλισμού που απαιτείται να συμμορφώνονται με τις απαιτήσεις:
  - Art. 3(3) d : Εξασφάλιση προστασίας δικτύου→ Ραδιοεξοπλισμός συνδεδεμένος στο διαδίκτυο
  - Art. 3(3)e: Προστασία ιδιωτικότητας και προσωπικών δεδομένων του χρήστη και συνδρομητή: → Ραδιοεξοπλισμός που έχει τη δυνατότητα να επεξεργάζεται προσωπικά δεδομένα, συνδεδεμένος με το διαδίκτυο, παιδικής φροντίδας, παιχνίδια και φορέσιμο εξοπλισμό
  - Art. 3(3)f: Προστασία από απάτη→ Ραδιοεξοπλισμός με δυνατότητα μεταφοράς χρημάτων, νομισματικής αξίας ή εικονικού νομίσματος

- Τεκμήριο Συμμόρφωσης για ραδιοεξοπλισμό που συμμορφώνεται με εθελοντικά εναρμονιστικά πρότυπα με σκοπό τη διατύπωση λεπτομερών τεχνικών προδιαγραφών των εν λόγω απαιτήσεων
- Οι προδιαγραφές θα εξετάσουν και θα αντιμετωπίσουν το επίπεδο των κινδύνων που αντιστοιχούν στην προβλεπόμενη χρήση κάθε κατηγορίας ή κλάσης ραδιοεξοπλισμού

Cyber Resilience Act (προϊόντα με ψηφιακά στοιχεία) θα αντικαταστήσει το RED Delegation Act και θα κτίσει πάνω σε αυτά τα πρότυπα

CEN/CLC/JTC13/WG8 Special WG RED SR

- ***Αίτημα Τυποποίησης προς CEN and CEN CENELEC***
- ***10 Ομάδες για τα 3 Εναρμονισμένα Πρότυπα***
- ***Το ελάχιστο απαιτούμενο περιεχόμενο των τεχνικών προδιαγραφών για τις ειδικές απαιτήσεις (specific requirements)***

Team	Requirement
1(+2?)	[D] Include elements to monitor and control network traffic, including the transmission of outgoing data • Jean-Paul van Assche - AT (NEN) • Jonathan Choudhury - AT (NEN) • Markus Wuensche - Eaton (CLC TC65x) • Carlos Valderrama - Huawei (UNE) • Ahmed Kasttet - Birdz (AFNOR)
2(+1?)	[D] is designed to mitigate the effect of ongoing denial of service attacks • Jens Guballa - Bosch (DIN) • Judith Rossebo - ABB (CLC TC65x) • Kilian Mitterweger - BSI (DIN) • Ralf Rammig - Siemens (DIN)
3	[D] [E] [F] implement appropriate authentication and access control mechanisms • Wolfgang Stadler - SICK (CLC TC121A) • Thomas Gilles –BSI (DIN) • Kai Wollenweber - Siemens (CLC TC65x) • Jean-Paul van Assche - AT (NEN) • Jonathan Choudhury - AT (NEN) • Maria Raphael – (CYS) • Ahmed Kasttet - Birdz (AFNOR)
4	[D] [E] [F] are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly know exploitable vulnerabilities as regards harm to the <d><e><f> • Ingo Hanke - SMA (DIN) • Octavian Popescu - EUCOM (NBN) • Lola Fernández - Knorr-Bremse • Constantinos Tsiourtos - CYS • Samim Ahmadi - Umlaut (DIN)
5	[D] [E] [F] are provided, with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities, that if exploited may lead to <d><e><f> • Torben Markussen - Kamstrup (DS) • Jacob Hansen - Kamstrup (DS) • Piotr Polak - Signify (NEN) • Ralf Rammig - Siemens (DIN) • Stiepan Kovac - QRC Eurosmart SA (ILNAS) • Simon Dunkley - Itron (BSI)

Team	Requirement
6	[D] [E] [F] protect the exposed attack surfaces and minimise the impact of successful attacks • Helene Sigloch - BSHG (DIN) • Benoît Stockbroeckx - Euralarm • Mariela Pavlova - Infineon (DIN) • Kai Wollenweber - Siemens (CLC TC65x) • Olivier Van Nieuwenhuyze - STMicroelectronics (NBN) • Stefan Korff - Miele (DIN)
7	[E] [F] protect stored, transmitted or otherwise processed <e><f> against accidental or unauthorised storage, processing, accesss, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e><f> • Gisela Meister - Eurosmart (DIN) • Meinhard Bohlen - Schneider Electric (TC205) • Jasja Tijink - ASFiNAG • Stiepan Kovac - QRC Eurosmart SA (ILNAS) • Rachel Menda-Shabat - Winbond Technology • Mariela Pavlova - Infineon (DIN) • Roland Atoui - Red Alert Labs (AFNOR) • Rainer Becker - Bosch (DIN) • Ahmed Kasttet - Birdz (AFNOR) • Georg Stütz - NXP (ASI)
8	[E] Include functionalities to inform the user of changes that may affect data protection and privacy • Rusne Juozapaitiene - ANEC • Peter Dickman – Google (SNV) • Maria Raphael - CYS • Santosh Sharman - KIWA (NEN) • Stefan Korff - Miele (DIN)
9	[E] [F] log the internal activity that can have an impact on <e><f> • Alex Buchan - DTG (BSI) • Stefano Ruffini - Bticino (UNI) • Philippe Magneron - Hager Group (AFNOR) • Jeppe Pilgaard Bjerre – (DS)
10	[E] allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information • Jacob Hansen - Kamstrup (DS) • Axel zur Muehlen - Schneider Electric • Hendrik Decroos - InfoSentry (NBN) • Stiepan Kovac - QRC Eurosmart SA (ILNAS)

2023: CEN/CLC/JTC13/WG8 Special WG RED SR

Meeting	Location	From		Till		Convenor	Secretariat
15	Online	Tuesday	2022-11-08			Ben Kokx	AdH, RC
~~16~~	~~Online~~	~~Thursday~~	~~2022-11-10~~			~~Kai Wollenweber~~	~~AdH, RC~~
17	Online	Tuesday	2022-11-15			Ben Kokx	AdH, RC
18	Online	Thursday	2022-11-17			Ben Kokx	AdH, RC
19	Online	Tuesday	2022-11-22			Ben Kokx	AdH, RC
20	Online	Thursday	2022-11-24			Ben Kokx	AdH, RC
21	Online	Tuesday	2022-11-29			t.b.d.	AdH, RC
22	Online	Thursday	2022-12-01			Judith Rossebo	AdH, RC
23	Delft (Hybrid)	Monday	2022-12-05	Friday	2022-12-09	Ben Kokx	AdH, RC
24	Oslo (Hybrid)	Monday	2023-01-16	Friday	2023-01-20	Ben Kokx	RC

RED Delegated Regulation hENs			
Stage Code	Stage	Target date	Duration
10.99	Decision on WI Proposal	2022-10-14	
			+ 16 weeks
20.60	Circulation of 1st WD	2023-02-03	
			+ 8 weeks
30.99	Acceptance of ENQ draft	2023-03-31	
			+ 3 weeks
40.20	Submission to Enquiry	2023-04-21	
			+ 12 weeks
40.60	Closure of Enquiry	2023-07-14	
			+ 8 weeks
45.99	Acceptance of FV draft	2023-09-08	
			+ 3 weeks
50.20	Submission to Formal Vote	2023-09-29	
			+ 8 weeks
50.60	Closure of Formal Vote	2023-11-24	
			+ 2 weeks
60.55	DOR/Ratification	2023-12-08	
			+ 2 weeks
60.60	DAV/Definitive text available	2023-12-22	

CEN/CLC/JTC13/WG8 Special WG RED SR

Αίτημα Τυποποίησης προς CEN and CEN CENELEC

Part B. Specific requirements for the harmonised standards listed in Annex I

7. Requirements for all harmonised standards

7.1. The harmonised standards shall reflect the generally acknowledged state of art.

7.2. The technical solutions laid down in the harmonised standards shall be proportionate to the risk that they aim to address. The harmonised standards shall be drafted and revised by applying the iterative process of risk assessment and risk reduction.

Risk-Assessment Sub-Group

CEN/CLC/JTC13/WG8 Special WG RED SR

Αξιολόγηση Κινδύνου- Risk Assessment

https://europa.eu/youreurope/business/product-requirements/compliance/technical-documentation-conformity/index

Your Europe > Business > Product requirements > Product compliance > Technical documentation and EU declaration of conformity

Life and travel

Running a business | Taxation | Selling in the EU | Human resources | Product requirements | Finance and funding | Dealing with customers

ON THIS PAGE

Risk assessment

As a manufacturer, you are responsible for identifying all the **possible risks** your product could pose and **determine the applicable essential requirements**. This analysis **must be included in the technical documentation**. In addition, you will need to explain the ways in which you have addressed the risks identified to ensure that your product complies with the applicable requirements, for example, by **applying harmonised standards**.