CEN Reference: BT N 10704

Draft BT C46/2017

CENELEC Reference: BT156/DG10503/INF

Simultaneous circulation to CEN and CENELEC TECHNICAL BOARDS

BT by correspondence	**CENELEC Agenda item:**	7.2.10
For decision (CEN)	**Issue date:**	2017-03-22
For information (CENELEC)	**Deadline:**	2017-06-20

SUBJECT

Creation of the new CEN-CLC/TC 'Cybersecurity and data protection'

BACKGROUND

TO NOTE:

This proposal is circulated to CENELEC BT for information at this stage to allow sufficient time to consult the national stakeholders. A decision is expected to be taken at its 156BT meeting on 2016-05-31/06-01.

***

In March 2017, DIN submitted a proposal to CCMC for the creation of a new CEN –CENELEC Technical Committee with the following proposed title: 'Cybersecurity and data protection', for which details are provided in Annex 1.

The scope of this proposed Technical Committee would cover the development of standards for data protection, information protection and security techniques with specific focus on cybersecurity covering all concurrent aspects of the evolving information society, including organizational frameworks and methodologies (including IT management systems), data protection and privacy guidelines, processes and products evaluation schemes, smart technology, objects, distributed computing devices and data services.

The lack of interoperable solutions, practices (process standards) and trustworthy IT solutions are, among other, gaps affecting the single market. On this basis, cybersecurity was identified as one of the ICT Standardisation Priorities for the Digital Single Market and this proposal aims to address the growing demands for standards in this field.

Part of the work of the new Technical Committee will consist in identifying internationally recognised standards (namely ISO/IEC/JTC 1 'Information Technology') that are suitable for endorsement as European ones. For the relevant standards and in conjunction with CEN–CLC/BTWG 6 'ICT standardization policy', the committee will decided on a case-by-case basis either on identical adoption as EN ISO/ EN IEC or adoption as EN with additional/complementary requirements in order to fulfil European requirements deriving from European legislation (e.g. General Data protection Regulation (GDPR)).

Last but not least, the Proposal for a New Field of Technical Activity points out to the intention of DIN to integrate the work programme of CEN-CLC/JWG 8 'Privacy management in products and services'. By doing so, privacy management will not be restricted to Mandate M/530 but will be addressed to ICT in general. Further details will be agreed upon with the TC members at its first meeting.

By Resolution BT C75/2009, BT decided that both of the following criteria are to be met for acceptance of such a proposal for new work (in a new area):

- A two-thirds majority of the votes cast (abstentions not counted) are in favour of the proposal (or more);
- At least 5 members express commitment to participate.

As a consequence, BT Members are requested to state explicitly, by means of the commenting field provided in the BT-balloting tool, whether or not they are committed to participate in the work.

PROPOSAL(S)

CEN/BT,

- having considered the proposal for a new field of technical activity submitted by DIN as included in Annex 1 to BT N 10704;
- considering that the following members have expressed commitment to participate:
  - o <members>
- decides
  - to create a new Technical Committee, CEN-CLC/TC xx 'Cybersecurity and data protection' with the provisional scope as provided in Annex 1;
  - to allocate the Secretariat of CEN-CLC/TC xx 'Cybersecurity and data protection' to DIN.

2017-03-22 – AI

PROPOSAL for a NEW FIELD OF TECHNICAL ACTIVITY	
Date of circulation ……	**CEN/TC / SC** N …… (where appropriate)
Secretariat ……	**CENELEC/TC / SC** (Sec) …… (where appropriate)
Type of technical body proposed (TC / SC / BTTF)	**CEN-CLC/TC**

IMPORTANT NOTE: Incomplete proposals risk rejection or referral to originator.

☒ The proposer has considered the guidance given in Annexes 1 and 2 during the preparation

Proposal (to be completed by the proposer)

Title of the proposed new subject
(The title shall indicate clearly and unambiguously, yet concisely, the new field of technical activity which the proposal is intended to cover.)

Cybersecurity and Data Protection

Scope statement of the proposed new subject
(The scope shall precisely define the limits of the new field of technical activity. Scopes shall not repeat general aims and principles governing the work of the organization but shall indicate the specific area concerned.)

Development of standards for data protection, information protection and security techniques with specific focus on cybersecurity covering all concurrent aspects of the evolving information society, including:

- Organizational frameworks and methodologies, including IT management systems
- Data protection and privacy guidelines
- Processes and products evaluation schemes
- ICT security and physical security technical guidelines
- Smart technology, objects, distributed computing devices, data services

This includes identification and possible adoption of standards already available or under development which could support the EU Digital Single Market and different standardization requests and/or EC Directives/Regulations. If required these standards will be augmented by TRs and TSs. Special attention will be paid to ISO/IEC JTC 1 standards, but will not be limited to this. Other SDOs and international bodies will also be taken into account, such as ISO, IEC, ITU-T, IEEE, NIST or industrial fora.

For the relevant standards different options will be considered:

- Identical adoption as EN using for example Vienna/Frankfurt agreements.
- Adoption as EN with additional/complementary requirements, for example in order to fulfil European legal requirements.

Purpose and justification for the proposal.

The experience and the results of the CEN-CENELEC Cyber Security Focus Group (CSCG) made clear that cybersecurity is essential to achieve a Digital Single Market. Also data protection and privacy are major objectives of the digitization of the European economy. With the identical adoption of the ISO/IEC JTC 1 standards on digital forensics as ENs (EN ISO/IEC 27037, EN ISO/IEC 27038, EN ISO/IEC 27040, EN ISO/IEC 27041, EN ISO/IEC 27042, EN ISO/IEC 27043 and EN ISO/IEC 30121) following the recommendation of CSCG, the first step has been done.

Further on, the CEN-CENELEC BTWG06 on ICT Standardization Policy has described in its strategy in 2016 the need for adoption of selected international standards as ENs. Based on this strategy the CEN and CENELEC BTs approved a process on how to adopt JTC 1 standards using a well-defined selection mechanism.

The adoption of international standards might not be sufficient for fulfilling all standardization requests and/or EC Directives/Regulations. CSCG has discussed this issue and recommended the establishment of a

CEN-CENELEC TC as an entity to be able to develop the necessary TRs and TSs if needed. The General Data Protection Regulation (GDPR) is one example of EU Regulations where the identical adoption of international standards is not sufficient. Whereas these international standards focus on generic processes and mainly on technology, the EU Regulations require consensus on how these technologies have to be implemented in order to fulfil EU Regulations/Directives.

The TC will take into account the relevance of international standards for European stakeholders by identifying standards that should be adopted and/or augmented by TRs and TSs. Augmenting standards can be necessary to protect European customers against insecure technology and the loss of data sovereignty as well as to prepare the floor for highly secure IT products and services of the European economy.

The CSCG cannot develop standardization deliverables (EN, TR, TS). Therefore, CSCG recommended the establishment of the proposed TC.

Additionally, with the fast digitization and the implementation of converging technologies it is expected that the EU will issue standardization requests in order to harmonize standards on cybersecurity and data protection and at the same time take European interests into account.

Standardization in the field of data protection will also support EU policymakers in developing, customizing or harmonizing schemes requiring information protection within different market sectors and implementing the ICT Standardization Priorities for the Digital Single Market.

Is the proposed new subject actively, or probably, in support of European legislation or established public policy?

☒ **Yes** ☐ **No**

If Yes, indicate if the proposal is

▪ in relation to EC Directive(s)/Regulation(s):

- General Data Protection Regulation (GDPR); REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016,;
- Directive on security of network and information systems (NIS Directive); DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016

▪ in relation to other legislation or established public policy:

- EU Digital Single Market;
- European Agenda on Security

Proposed initial programme of work

Proposed **initial** programme of work for the TC (the final programme of work will be decided by the participants of the TC)

Title/definition	**Target dates**	**Deliverable**
Adoption of ISO/IEC JTC 1 standards as ENs	3 year timeframe	EN
Adoption of other international standards as ENs	3 year timeframe	EN
Development of TRs and TSs supporting the GDPR and based on international standards	3 year timeframe	TR or TS
Development of TRs and TSs supporting the NIS Directive and based on international standards	3 year timeframe	TR or TS
Guidelines and best practices for the European economy on how to implement international cybersecurity and data protection standards by fulfilling EU legislations.	3 year timeframe	TR or TS

As cybersecurity and data protection go hand-in-hand with privacy issues, the TC will further integrate the work programme of CEN-CENELEC JWG 8 “Privacy management in products and services”. By doing so, privacy management will not be restricted to Mandate M/530, but will be addressed for ICT in general. Further details will be planned with the participants of the TC.

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing CEN, CENELEC, ISO and IEC deliverables.
The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized. If seemingly similar or related work is already in the scope of other committees of the organization, or in other organizations, the proposed scope shall distinguish between the proposed work and the other work. The proposer shall indicate whether his or her proposal could be dealt with by widening the scope of an existing committee or by establishing a new committee.)

The new TC will consider the work of JTC 1 and other relevant SDOs and consider the possible adoption of their standards as ENs.

The focus is on standards developed by ISO/IEC JTC 1 as this committee is the entity that is responsible for the basic ICT standards of ISO and IEC. JTC 1/SC 27 “IT Security techniques” developed a series of standards on IT security techniques and is currently also drafting a standard on Data Protection Management System. The work of other JTC 1/SCs dealing with IT-security issues, e.g. SC 17 “Cards and Personal Identification” and SC 37 “Biometrics”, will also be considered by the new TC.

The following WIs currently assigned to CEN sub-sector F12 ‘Information Processing Systems’ due to lack of a corresponding TC will be reallocated to the new TC: EN ISO/IEC 27000, EN ISO/IEC 27001, EN ISO/IEC 27002, EN ISO/IEC 27037, EN ISO/IEC 27038, EN ISO/IEC 27040, EN ISO/IEC 27041, EN ISO/IEC 27042 und EN ISO/IEC 27043.

A listing of relevant existing documents at the international, regional and national levels.
Any known relevant documents (such as standards and regulations) shall be listed, regardless of their source, and should be accompanied by an indication of their significance.

The identification of existing standards that should be either identically adopted or augmented will be the first task of the TC.

Known patented items

☐ **Yes** ☒ **No** **If "Yes", see CEN-CENELEC Guide 8 and provide full information in an annex**

A simple and concise statement identifying and describing relevant affected stakeholder categories (including small and medium sized enterprises) <u>in particular those who are immediately affected from the proposal</u> (see Annexes 1 and 2**) and how they will each benefit from or be impacted by the proposed deliverable(s)**

- European Industry and commerce is shaped by small and medium sized enterprises (SME). This has to be taken into account when adopting international cybersecurity and data protection standards as ENs. The TC will prepare guidelines and best practices helping SME to establish high quality cybersecurity and data protection. For those who provide cybersecurity and data protection products and services, the harmonization of cybersecurity and data protection standards in Europe guarantees a huge market to enable product and service innovation and develop the EU home market as a reference for high-quality products and services at an international level.

- Governments play a leading role as a purchaser of IT technology. Further they prepare the infrastructure and maintain services for business and citizens. The past has proven that for EU wide IT projects that are not based on standards, a dissemination of these solutions will not happen. IT security and data protection are important topics of such projects. European standards will foster the use of standards in IT projects within the European Single Market. This is the basis for interoperability and the dissemination of solutions.

- Consumers need to be protected against products that do not fulfil IT security requirements, as it recently turned out to be the case for some devices such as surveillance cameras, smart home devices and wearable devices like wristbands. Incidents at the end of the year 2016 have shown that with a fast growing number of devices that are connected to the Internet, security gaps in some products are being exploited by hackers. Sensitive data can be accessed via these insecure devices. The implementation of ENs in the area of data protection will raise the quality of services and products in Europe.

As cybersecurity and data protection are essential functionalities of ICT products and solutions, all stakeholders are immediately affected by the implementation of ENs on cybersecurity and data protection.

Liaisons: **A listing of relevant external European or international organizations or internal parties (other CEN, CENELEC, ETSI, ISO and/or IEC committees) to which a liaison should be established (in the case of ISO and IEC committees via the Vienna or Frankfurt Agreements).** • CEN/TC 224 • ISO/IEC JTC 1 • ETSI TC CYBER • IEC/TC 65 • ISO/TC 292	**Joint/parallel work:** **Possible joint/parallel work with:** ☐ CEN (please specify committee ID) ☐ CENELEC (please specify committee ID) ☐ ISO (please specify committee ID) ☐ IEC (please specify committee ID) ☐ Other (please specify)

Name of the Proposer
(include contact details)

DIN Deutsches Institut für Normung e.V.
Am DIN-Platz
Burggrafenstrasse 6
10787 Berlin
Germany

Contact person:
Volker Jacumeit
Tel: +49 30 2601-2186
E-Mail: volker.jacumeit@din.de

An expression of commitment from the proposer to provide the committee secretariat if the proposal succeeds.

After consultation of national and European stakeholders, DIN is prepared to provide the committee secretariat.

Signature of the proposer

German CEN/BT Member

Annex(es) are included with this proposal (give details)

☐