ICDPPC Global Privacy and Data Protection Awards

2018

Entry Form

Deadline 29 June 2018

To submit an entry to the ICDPPC Global Privacy and Data Protection Awards please complete and email this form to ExCoSecretariat@icdppc.org no later than 29 June 2018.

Note: ICDPPC member authorities can submit as many entries as they wish but a separate form should be used for each different entry. Please complete the entry in English.

1. **Contact details for this entry**:
    a. Name and email address of person completing this form:
    b. Name of Data Protection or Privacy Authority: The Norwegian Data Protection Authority

2. **Eligibility**: By submitting this entry I confirm that:
    a. The Authority is a member of the International Conference of Data Protection and Privacy Commissioners.
    b. The initiative described in this entry was undertaken since the last edition.
    c. I am aware that the information in the entry (other than the contact details in 1(a) above) will be publicised by the ICDPPC Secretariat.

3. Please indicate which **category or categories** you wish to enter (delete those that do not apply; you can enter multiple categories):
    a. Education and public awareness
    b. Accountability
    c. Dispute resolution and enforcement
    d. Innovation
    e. People's Choice

4. **Description of the initiative**
    a. Please provide a brief summary of the initiative (no more than 75 words):

Software development with Data Protection by Design and by Default
We have developed these guidelines to help organizations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others. These guidelines are primary intended for developers, software architects, project managers, testers, data protection officers and security advisors.

    b. Please provide a full description of the initiative (no more than 350 words):

Software development begins with an idea of creating a product that will simplify or improve the quality of a process or task. How the software will solve the task is described in functional requirements.

Software development methodology comprising basic activities which ensure that the final product is robust. Norwegian DPA's guidelines comprising the key activities to ensure that the final product also is data protection by design and by default, illustrated by a circular diagram because both software development and safeguarding privacy are continuous processes.

The guide start with **training**. In the section on training, we cover the most important topics on which to provide training, why, how to do this, and which tools to use.

The section on **requirements** describe the measures needed to ensure data protection and security, the tolerance levels the organisation should set for data protection and security, and the need to assess both security risks and data protection implications.

The next section takes these requirements further, to **design**, by dividing them into data oriented and process oriented design requirements. During this activity, it is important that the organisation carries out both threat modelling and an analysis of the attack surfaces.

The **coding** activity underlines the importance of developers using approved tools and frameworks, disabling unsafe functions and modules, and regularly carrying out static code analysis and code review.

The section on **testing** involves a recommendation to test whether data protection and security requirements are implemented properly, a description of what sort of security testing should be carried out, and an explanation of the importance of threat modelling and analysing the attack surface.

Before **release**, an incident response plan should be established, and a full security review of the software should be carried out. Release is then approved and all relevant data from the entire development process are archived.

The final activity involves the **maintenance** of the software and the response to incidents. The organisation should be prepared to respond to incidents, personal data breaches, faults and attacks, and be capable of issuing updates, guidelines, and information to users and those affected by the software.

c. Please explain why you think the initiative deserves to be recognised by an award (no more than 200 words)

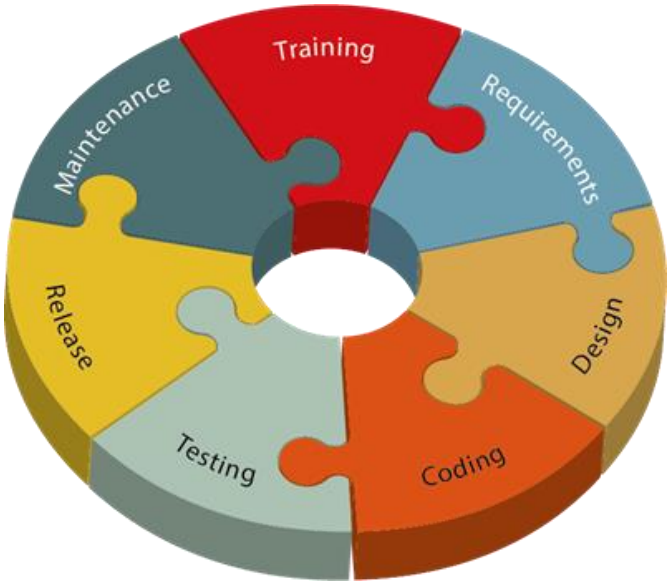
The guidelines have to be specific and clear so that organisations that develop software, applications, services, systems etc. and follow the guide, and later on can get their processing activities certified and get a privacy seal or mark according to article 25 (3).

The framework is not meant to be a substitute for a company's methodology for software development, but it is a supplement to ensure that privacy and security are included in the methodology.

There is abundant technical literature that focuses on security by design when developing software. Relatively little has however been written about data protection by design and by default when developing software. While working on this guide, we have used Software Development LifeCycle (SDLC), Microsoft Security Development Lifecycle (SDL) and ENISA; Privacy and Data Protection by Design – from policy to engineering, as a starting point, and explored how to incorporate privacy principles, subject rights, and the requirements of the GDPR into every step of the process.

The guidelines has already become a gold standard for developers and adopted by three universities in Norway. We think it is because the guide is specific, clear and have checklists that can be used directly by the different developer professions.

Include a photograph or image if you wish (note this will help illustrate the description of the entry on the ICDPPC website; the image can be pasted into the entry or send as an attachment or a link may be provided):



d. Please provide the most relevant link on the authority's website to the initiative (if applicable) (The website content does not need to be in English):

https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/

e. Please provide any other relevant links that you wish that help explain the initiative or its impact or success (e.g. links to news reports or articles):
https://event.dnd.no/fmhdnd/lansering-av-datatilsynets-veileder-for-innebygd-personvern/
https://vimeo.com/233819047
https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2018/vinner-av-innebygd-personvern-i-praksis-2017/

https://www.isf.no/datatilsynets-fagseminar-premieutdeling-innebygd-personvern-praksis/
http://iresponse-rri.com/2018/privacy-by-design
https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2018/konkurranse-innebygd-personvern-i-praksis-2018/konkurranse-innebygd-personvern-i-praksis-2018/
https://fpf.org/gdpr/
http://www.cw.no/artikkel/personvern/kjernejournal-vant-personvern-pris
https://www.regjeringen.no/no/dokumenter/meld.-st.-16-20172018/id2605023/sec2
https://infosec.sintef.no/stikkord/innebygd-personvern/
https://3min.io/hva-er-innebygd-personvern-og-hvordan-få-det-inn-i-utviklingsløpet-edbfcf2180eb
https://ehelse.no/Documents/Normen/Presentasjoner/Normkonf2017/2017-11-30-%20Workshop%20Normkonferanse.pdf
https://www.uio.no/tjenester/it/sikkerhet/lsis/tillegg/inneperson.html
https://www.mn.uio.no/ifi/studier/masteroppgaver/cybersecurity/innebygd-personvern-i-app-utvikling.html
https://www.mn.uio.no/ifi/studier/masteroppgaver/cybersecurity/innebygd-personvern-i-maskinlering.html