5th NIS Platform Plenary 27.5.2015 – Group discussions on how voluntary information sharing for network and information security purposes interacts with data protection

Introduction

At the 4thPlenary 27.11.2014 the NIS Platform community made strong calls for addressing data protection in the context of cybersecurity information sharing.

This discussion paper is used as background for group discussions during the 5th NIS Platform Plenary 27.5.2015.

The scope of NIS Platform discussions is currently on voluntary information sharing, hence mostly private-to-private. This discussion paper will show how general data protection rules apply to such situations. Whereas exemptions or specific authorisations, in the public interest, would usually apply when notifying national authorities of network and information security incidents, such legal bases are not explicit for situations of private-to-private sharing of information for cybersecurity preventive purposes. In the absence of specific rules, any guidance should be based on the interpretation of general data protection principles enshrined in EU and national data protection rules (e.g. anonymisation of data; lawfulness, proportionality and time limitation; documentation of procedures for ex-post audit).

The aim of the group discussions is to scope the topics as narrowly and precisely as possible, based on the needs expressed by the NIS Platform community.

Questions to be discussed in groups during the NIS Platform Plenary:

- How to illustrate use cases/scenarios of voluntary information sharing including personal data? Such scenarios should clearly show:
    - the actors involved (who is exchanging info and with whom),
    - the types of personal data,
    - the purpose of the processing of personal data,
    - the means of data exchange.
- Possible legal bases to justify voluntary information sharing efforts on the basis of EU data protection legislation (Article 7, Directive 95/46): legitimate interest, public interest, legal obligations?
- Examples of existing technical solutions & security controls that could reduce the risk of personal data disclosure and loss during processing (such as data minimization, pseudonimisation/anonymisation, etc)?

Expected outcome

The outcome of the group discussions should be exploratory and high-level, since DG CNECT is not in the lead for all of these strands, but the topic is nonetheless important for cybersecurity and NIS policy.

Based on the outcome a short one-page section on links between voluntary information sharing and data protection could be inserted to Chapter 3. Should the group discussions lead to the conclusion that further work and analysis is needed a dedicated work stream could be initiated under WG2, with more flexible timeline than the current set of guidance documents that the NIS Platform is working on for 2015.

NIS Directive

The proposed NIS Directive[1] would not directly apply in private-to-private information sharing; it would only apply in private-to-public situations when market operators notify significant network and information security incidents to national authorities (Art 14). Processing of personal data for such purposes should be considered in the *public interest* (Article 1.6). The NIS Platform will come back to identifying good practices for such private-to-public sharing of information in Chapter 5 'Mandatory incident notification', with the help of ENISA[2], once the NIS Directive has been adopted.

General Data Protection Rules

The general EU data protection Directive[3] applies to anyone handling personal data, either as a controller or processor, and is applicable in situations of sharing information for network and information security purposes in particular to the extent that such sharing entails the processing of personally identifiable information (Article 1 and 2); and requires that appropriate technical and organisational measures be taken to secure the data from unauthorised access during processing (Article 17). The Directive requires, among others, that data should be processed fairly and lawfully; collected only for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; not be disproportionate nor kept longer than necessary. The processing can take place only on the basis of one of the specific legal grounds for processing is fulfilled. Such legal bases include, in particular, consent of the data subject (Article 7.a), processing necessary for fulfilling a contractual obligation (Article 7.b), complying with a legal obligation (Article 7.c), to perform a task in the *public interest* (Article 7.e) or for the purposes of a legitimate interest (Article 7.f). Transfer of data to third countries is in principle allowed only if the level of protection in the third country is considered adequate, if specific exceptions apply or other specific adequate safeguards are ensured.

An update of the Directive is currently ongoing through the proposal for General Data Protection Regulation (GDPR)[4]. Among the various important proposed changes, this proposal would require that controllers notify personal data breaches to supervisory authorities (Article 31), and to the data subject concerned (Article 32), unless the data was protected by sufficient technical protection measures (encrypted). A processor shall alert and inform the controller immediately after the establishment of a personal data breach.

The GDPR proposal contains recital 39 that is specific to network and information security:

> *The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution*

[1] COM (2013)48

[2] This work will draw upon ENISA experience gained under Article 13a of E-Communications Regulatory Framework Directive 2002/21 (as amended by Directive 2009/140) and Article 4 of ePrivacy Directive 2002/58.

[3] Directive 95/46

[4] COM(2012)11

and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

ePrivacy Directive

The requirement to notify personal data breaches to relevant authorities, and in certain cases also to the subscribers and individuals concerned, already applies for publicly available electronic communications services (telecom operators and Internet service providers) according to Article 4 of the ePrivacy Directive[5].

The Commission is empowered to adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements, and such rules have been adopted in 2013[6].

Article 29 Working Party

Under Article 29 of General Data Protection Directive 95/46 a Working Party has been set up, which consists of the European Data Protection Authority (EDPS), national Data Protection Authorities (DPAs), and the Commission acting as a secretariat (DG JUST). It examines any question covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures, and also of questions arising under the ePrivacy Directive . It has a specific technology subgroup which regularly discusses IT and data protection related topics. The Working Party has issued several opinions that are of interest for network and information security information sharing, such as for example those on the notion of personal data; anonymisation; consent. Some examples of opinions expressed include:

- Personal data: identification numbers, location data, IP-addresses, online identifiers or other specific factors relating to an individual should be considered personal data. This has also been confirmed by the European Court of Justice.

- Anonymisation: where a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. However, it is clear from case studies and research publications, and the Opinion of the Article 29 Working Party, that the creation of a truly anonymous dataset from a rich set of personal data, whilst retaining as much of the underlying information as required for the task, is not a simple proposition. For example, a dataset considered to be anonymous may be combined with another dataset in such a way that one or more individuals can be identified.

- Appropriate technological protection measures: a confidentiality breach on personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified to the authority. Nevertheless, if the confidentiality of the key is intact, the data are in principle unintelligible to any person who is not authorised, thus the breach is unlikely to adversely affect the data subject and therefore doesn't need to be notified to the data subject.

- Consent: should as a general rule be given before the processing starts. The Directive clearly presents consent as a ground for lawfulness[7]. Clarifying the relation of consent with the

[5]Directive 2002/58

[6] Commission Regulation 611/2013

[7] Consent is derived from several Member State laws and traditions, and reflected in the EU Directive, but not generally appearing outside the EU.

other grounds of lawfulness - e.g. in relation to contracts, tasks of public interest or legitimate interests of the controller, and the right to object - will help to highlight the role of consent in specific cases. Article 7 starts with consent, and goes on to list the other grounds, including contracts and legal obligations, moving gradually to the balance of interests. It should be noted that the five other grounds following consent require a "necessity" test, which strictly limits the context in which they can apply. In some transactions a number of legal grounds could apply, at the same time. In other words, any data processing must at all times be in conformity with one or more legal grounds. This does not exclude the simultaneous use of several grounds, provided they are used in the right context. Some data collection and further processing may be necessary under the contract with the data subject – Article 7(b); other processing may be necessary as a result of a legal obligation – Article 7(c); the collection of additional information may require separate consent – Article 7(a); still other processing could also be legitimate under the balance of interests – Article 7(f).

Example: buying a car
The data controller may be entitled to process personal data according to different purposes and on the basis of different grounds:
- Data necessary to buy the car: Article 7(b),
- To process the car's papers: Article 7(c),
- For client management services (e.g. to have the car serviced in different affiliate companies within the EU): Article 7(f),
- To transfer the data to third parties for their own marketing activities: Article 7(a).

A questionnaire to national CSIRTs has been circulated by Article 29 Working Party, but not yet resulted in any guidance or opinion.

ENISA

Extract from ENISA report 'A flair for sharing – encouraging information exchange between CERTs'[8]:

Appendix A: Example legal checklist for privacy and data protection

From a practical perspective, CERTs that are looking to share or request information should at the very least evaluate the following questions with respect to data protection:
☐ Is the information legally considered to be personal data, and therefore subject to data protection rules?
☐ If so, have you obtained the personal data legitimately, i.e. in accordance with nationally applicable data protection laws? The CERT will need to evaluate in particular:

o Whether there was a legitimate basis for the collection of the personal data. This question should be evaluated keeping into account the original source of the data (e.g. an ISP or service provider), the specific mandate of the CERT and any legal basis for its work (including possible specific laws or legal exemptions);
o Whether there are specific national legal restrictions that apply to the data, e.g. protection of judicial data, professional secrecy or telecommunications secrecy;
o Whether the collected data observes the principles of the nationally applicable data protection laws, including specifically with respect to data quality and proportionality. The use of anonymisation and encryption techniques should be considered whenever viable.

[8] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

o Whether data subject rights are appropriately respected, again taking into account any specific laws that may apply to the CERT.
☐ Before requesting personal data from a third party or examining whether or not to share personal data with a third party, the CERT should:

o If this is not the case, it should examine whether an alternative basis for legitimacy exists, on the basis of the national transposition of Article 7 of the Data Protection Directive. For this question, the specific mandate of the CERT and any legal basis for its work is crucial, as is the identity, mandate and legal basis for the third party's operations;
o Evaluate whether data will be transferred to a recipient outside of the European Union, and if so, whether this transfer is legitimate on the basis of the national transposition of Article 25 of the Data Protection Directive;
o Verify whether the planned data exchange observes the principles of the nationally applicable data protection laws, including specifically with respect to data quality and proportionality. The use of anonymisation and encryption techniques should be considered whenever viable;
o Obtain assurances that the recipient of the shared data will only process it in accordance with applicable data protection law.
If no legal expertise is available in-house, the CERT should consult appropriate third parties such as lawyers or data protection bodies before processing personal data.