Governance of data related to offensive security and blue team

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Governance in terms of data related to offensive security and blue team entails setting-up internal policies and procedures for implementation of proper mechanisms and legal requirements concerning:

i. Gathering of personal data and sharing such data with third parties that are either private entities or authorities.
ii. Managing whistleblowing filings concerning data processing and information security
iii. Proper collection and preservation of evidence in case of security incidents

Thus, a company may collect, process and transfer data during the phase for choosing and implementing proper security measures and during the phase of security incident analysis.

The below sections outline the main legal requirements and legal risks to be taken into account by the company, together with specific methodologies that can be implemented by the company.

1. Governance of personal data in interaction with third parties and authorities

In terms of international cooperation concerning cyber security, EU member states have been cooperating among themselves and with the US since 2010 on a joint approach on certain points, such as establishing standard good practices, incident handling procedures and raising awareness of cyber threats.[1] As outlined in this section, these types of initiatives can be further detailed in order to ensure proper and consistent implementation between stakeholders involved in the data sharing.

Further, cyber security has been on the agenda of the EU in the past decade. In 2017 the strategy of the EU in this respect has been mentioned by way of several impact assessments, draft legislation and communications. These documents essentially mention four ways forward: (i) more cooperation among member states and on an international level in terms of preventive steps to be taken, (ii) immediate cooperation among members states and on an international level in case of cyber-attacks, (iii) raising awareness on cybercrime matters, and (iv) enhanced research and development in the cyber security field and ensuring a greater number of specialists in this field.[2] These four ways forward, implemented in a cyclical and comprehensive manner by multiple stakeholders at an international level lead, in time, to an increase in the maturity level of information security in companies.

The cooperation on cyber-attacks and, consequently, on preventive steps against cyber-attacks has proven over the last decades as essential in growing the level of information security. This becomes more useful as the number of entities participating in the cooperation grows in terms of sectors of activity and territorial location. This constant cooperation from an early stage of cyber-attack identification can decrease the time until characteristics for identification of cyber-attack are established

[1] European Commission, *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats*, 2011, http://europa.eu/rapid/press-release_MEMO-11-246_en.htm , last accessed on 22 December 2019.

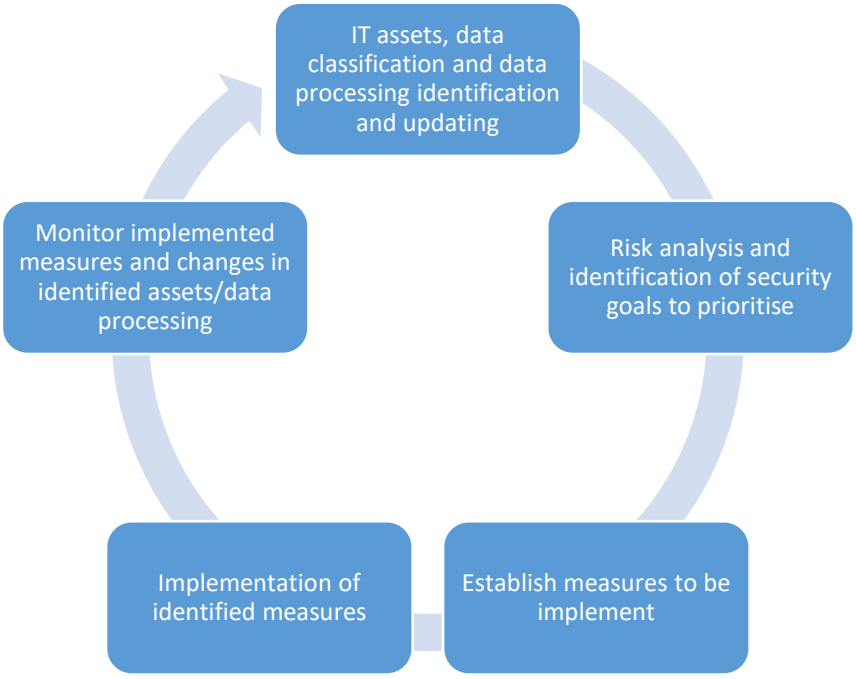
[2] Joint Communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, September 2017. Commission Recommendations (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

and efficient preventive measures are identified. Constant cooperation, in time, leads to an increase into the research on cybercrime and cyber security and, subsequently, in the increased need for cyber security specialist individuals.

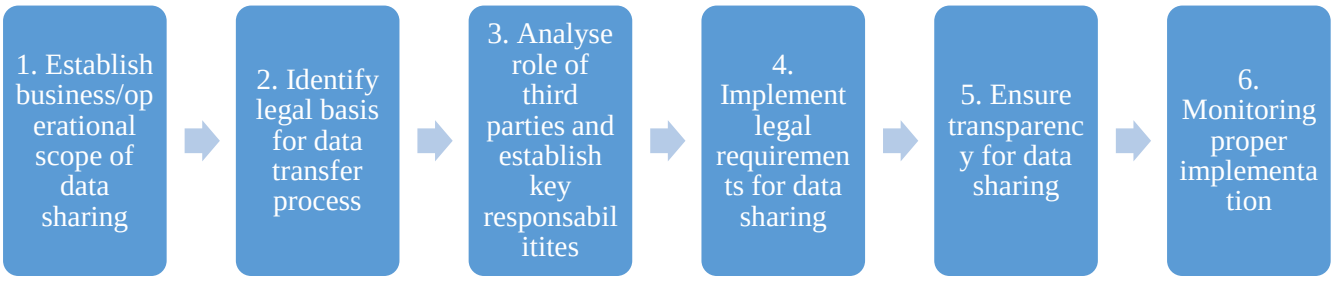
Nevertheless, in order to implement an efficient cooperation and ensure the implementation of preventive steps, the actual end-users have to be aware on the one hand about the cybercrime techniques and, on the other hand, about the preventive steps to be taken to ensure information security.

Data protection requirements generally stem from legal provisions, which either mention a principle for data processing or detailed provisions to be implemented. In any situation, even if data protection entail compliance with legal requirements, in order to proper implement this in a company, a data governance framework has to be implemented. There are various approaches in this respect, from the NIST Privacy Framework to ISO 27701 on privacy information management.

A data governance model used by a company should cover certain main steps and actions to be taken by the company. We detail below a data governance model that includes steps for both data protection and information security:

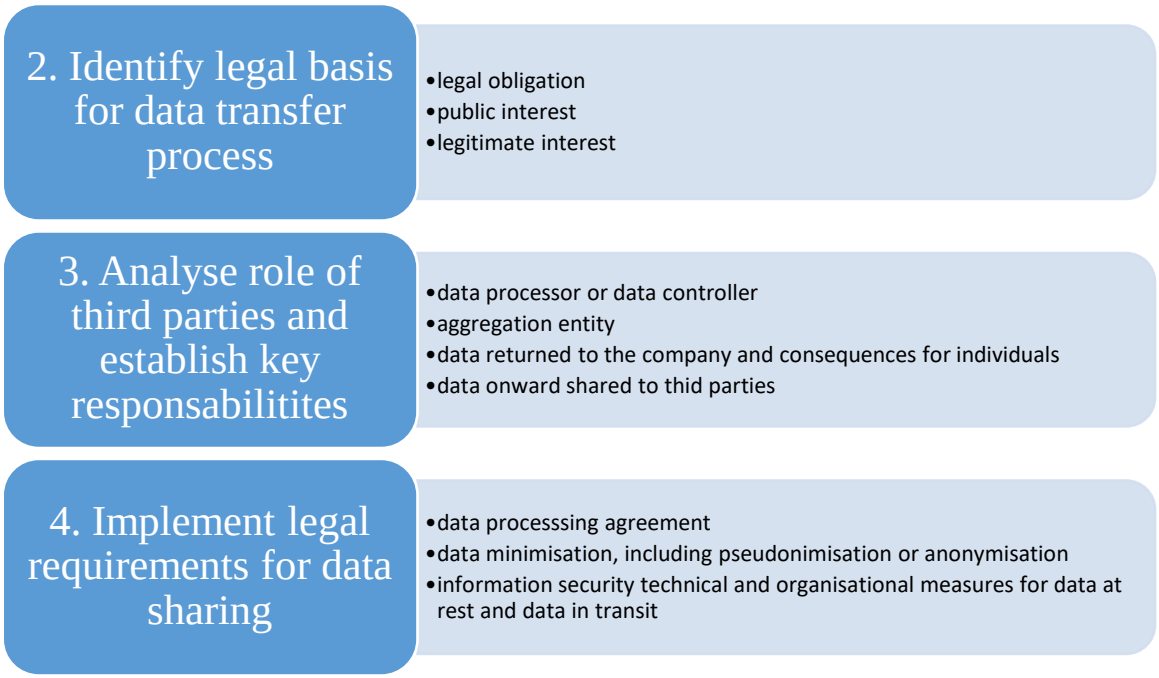


Within the above data governance context, in terms of transfer to third parties, we outline below a specific data governance model that can be integrated in the overall data governance framework of the company, while maintaining the specifics in case of third party involvement. The approach we propose includes the following main steps in the data governance and can be applied for scenarios referring to data shared by the company and data received by the company. Further, each step outlined in this model contains data protection, legal and security requirements.



The first step mentioned above starts with the business/operational need identified in this case by the IT/Information security department. Steps 2, 3 and 4 involve the cooperation of the data protection, legal, IT and information security departments in order to ensure proper compliance with legal requirements and sharing of data useful for the identified business/operational scope, with each department outlining requirements impacting the sharing process which are relevant from their perspective. Step 5 is ensured by the data protection department together with the business department having contact with the individuals whose personal data is being shared.

This section outlines the below aspects for each steps of the data governance, with practical examples and aspects to be analysed.



The sharing of data for prevention purposes may be performed to multiple types of third parties.[3] The data can be shared within the same group of companies, with service providers that aggregate data

[3] The Global Cyber Security Capacity Center, *Computer Security Incident Response Teams(CSIRTs): An Overview*, 2014, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf , last accessed on 2 February 2020.

in order to determine trends in cyber-attacks, with an organisation for a sector in order to gather information about sector-wide potential attacks or with other third parties. Further, data may be sent to the entire supply chain in order to avoid supply chain attacks or to a particular entity providing forensic services (as the private entity that collected the data does not have necessary skills in this respect). In certain cases, due to the potential global coverage of a potential attack, sharing of data on a publicly accessible website may be contemplated.[4] Each case may have different implications in terms of legitimate interest for data sharing.

In this section we cover the main aspects to be analysed by the company in case of sharing of data about security incidents or about vulnerabilities with third parties.

In terms of legal obligations concerning sharing of data on security incidents[5] for IT systems, the NIS Directive is the main source of such obligations.[6] However, data protection legislation may also be considered relevant, as it entails state of the art security measures to be implemented for the confidentiality, integrity and availability of data and for the resilience of the organisation.

The NIS Directive[7] goes further and establishes national Computer Security Incident Response Teams (CSIRTs) and, on the other hand, a network of CSIRTs. [8] The CSIRTs within a country can be also private entities.

As an example, under Romanian law,[9] notifications of security incidents include generally details on the incident, impact of the incident and preliminary measures adopted. The law expressly mentions that no data bringing negative consequences on the rights and liberties of individuals/third parties involved in the incident should be provided.[10]

On the one hand, the notification obligations[11] are useful in terms of sharing information and correlated these in order to identify patterns and prevent future attacks.

On the other hand, information granted concerning security incidents/data breaches should be limited in terms of access and content, in order to be in compliance with applicable legal requirements. For instance, confidential information should not be included in the notification sent to the data subjects, but limit the data disclosed to the minimum requirement under the law.[12] Such information may be used

---

[4] Hewling, Moniphia, *Cyber Intelligence: A Framework for the Sharing of Data*, International Conference on Cyber Warfare and Security, 2018.

[5] Article 14 of the NIS Directive.

[6] Erich Schweighofer, Vinzenz Heussler, Peter Kieseberg, *Privacy by design data exchange between CSIRTs*, Annual Privacy Forum, 2017.

[7] Articles 9 and 12 of the NIS Directive.

[8] The White House, Fact Sheet: Cyber Threat Intelligence Integration Center, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center , last accessed on 1 February 2020.

[9] Article 27 of law 362/2018 implementing the NIS Directive.

[10] Luis Tello-Oquendo et al, *A Structured Approach to Guide the Development of Incident: Management Capability for Security and Privacy*, https://pdfs.semanticscholar.org/023e/d70a52d6c8396e463188be7ddd88544869ec.pdf , last accessed on 2 February 2020.

[11] Hong, Seung-Hun and Alazab, Mamoun, Cybercrime and Data Breach: Privacy Protection through the Regulation of Voluntary Notification (2017). Prepared for the Korea Legislation Research Institute (KLRI), 2017 Legal Scholar Roundtable, How Law Operates in the Wired Society, Seoul, Korea, 2017. https://ssrn.com/abstract=3042174 , last accessed on 28 February 2020.

[12] Dähn, Marie-Christine and Pernice, Ingolf and Pohle, Jörg and Goldman, Zachary and Nemitz, Paul Friedrich and Christakis, Theodore and Milch, Randal S. and Kent, Gail and Wetzling, Thorsten Manuel and von Lewinski, Kai and Djeffal, Christian and Herpig, Sven and Krüger, Philipp S. and Grafenstein, Maximilian and Barker, Tyson and Rubinstein, Ira and Lenssen, Klaus and Gitter, Rotraud, Privacy and Cyber Security on the Books and on the Ground (August 1, 2018). Edited volume. Berlin: Alexander von Humboldt Institute for Internet and Society. ISBN: 978-3-9820242-1-9. https://ssrn.com/abstract=3250354 , last accessed on 28 February 2020.

by the perpetrator or other individuals in order to identify vulnerabilities in the system of the company that incurred the security incident (additional information may be obtained through data subject access requests).[13] Further, information about the perpetrator may be contained in the notification and this may not need to be available to data subjects, but only to the authorities assisting in the investigation and monitoring of the security incident.

Nevertheless, in some cases, it may useful to share information even about an unsuccessful attack.[14] Although not expressly mentioned as a legal obligation in practice, the data gathered during the attack or in case of active security measures may be useful for prevention of further attacks.

As a general note, in case of transfer between data controllers who act independently, each data controller has the obligation to fulfil its own legal requirements as data controller. Thus, each data controller has to ensure that the sent data is transferred based on a legal basis and in accordance with legal requirements.[15] In addition, each data controller has to ensure that the data is received based on a legal basis and in accordance with legal requirements. Thus, a data controller cannot assume that the data it receives is in accordance with legal requirements without verifications in this respect.

For sharing of data between such independent data controllers, usually, in the agreements between them, there are specific clauses that ensure that the data sender has taken specific steps to comply with data protection requirements upon collection of the personal data and, usually, that it has also informed the data subjects about the transfer to the data receiver.[16] Sometimes, the data sender undertakes to perform the information obligation on behalf of the data receiver, as it has direct contact with the data subject.

In the case of joint controllers,[17] matters relating to transparency about data sharing should be discussed and agreed between the joint controllers. For the sharing of threat information, as the data is useful for the common purpose of all entities involved, it may be argued that these act as joint controllers. In such case, the liability of each of them should be detailed in the data sharing agreement between them, including any limitations of future uses of received data. Thus, matters relating to liability of each data controller (independent or joint controllers) can be detailed in the contractual documentation.

In case of threat data sharing, depending on the structuring of the data sharing, the entities participating in the system may be joint controllers or independent controllers. This is relevant from a liability perspective.

---

[13] ECJ, College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer, C-553/07, 7 May 2009, concerning the right of access of the data subject. Bucharest Court of Appeal, decision no. 158/2019.

[14] ENISA. 2014. Standards and tools for exchange and processing of actionable information. (Nov. 2014). https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport , last accessed on 28 February 2020. Maria Bada et al., Computer Security Incident Response Teams (CSIRTs) An Overview, Cybersecurity Capacity Portal, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/computer-security-incident-response-teams-csirts-overview , last accessed on 28 February 2020. ENISA. 2011. A air for sharing - encouraging information exchange between CERTs. (Dec. 2011). https://www.enisa.europa.eu/publications/legal-information-sharing-1/at_download/fullReport , last accessed on 28 February 2020.

[15] NIS Cooperation Group, *Reference document on security measures for Operators of Essential Services, CG Publication 01/2018.*

[16] Bucharest Tribunal, decision no. 182/2019 concerning the legal obligation of fiscal authorities concerning the public disclosure of receivables. Bucharest Tribunal, decision no. 4925/2019 concerning having a protocol between prosecution unit and land book registry as basis for data transfer.

[17] Hongxin Hu, *Detecting and resolving privacy conflicts for collaborative data sharing in online social networks*, ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference, pages 103-112.

The main data protection risks are related to transparency and legal basis for transferring. Lack of these aspects may result in sanctioning with fines for one or both of the data controllers.[18]

The data gathered for monitoring of device activity for preventing cyber-attacks and fraud should not be used for subsequent / other purposes. This ties in with the net neutrality discussions over the last decade.[19] These mainly refer to ISPs (especially given their deep packet inspection capabilities), but are also applicable to other companies that have access to large amounts of data about individuals (as is the case of applications that scan and monitor devices for threats), especially in case such data is shared with third parties or aggregated in a single central database.[20] The implementation of the need to know and data minimisation principles under data protection legislation is essential in this respect, both in terms of the aggregated database containing the data and also by each company that has access to such data. This also assists in ensuring compliance with article 8 of the ECHR (European Court of Human Rights).

Transparency aspects

The transparency principle entails that the data controller informs the data subject in a clear, concise and easy to understand manner of the data processing and data sharing. In case consent is required for the data sharing, the information is performed prior to obtaining the consent of the data subject. This is relevant also for the criminal law analysis in terms of the conditions for validity of the consent exemption to be fulfilled.

Interesting in case of data sharing between two data controllers is the manner in which the receiving data controller performs its information obligation towards the data subject. Whereas the data sender may have collected the data directly from the data subject, the data receiver generally has obtained indirectly the personal data (and may not be in direct contact with the data subject). Usually, in practice, as per an agreement between the data sender and data receiver, the data sender provides the needed information notice on behalf also of the data receiver.

Data protection authorities in member states[21] have commenced to express their opinion that a complete list of data receivers has to be provided to individuals (irrespective of whether consent is needed or not for the data sharing). This impact also the manner in which data subject requests are dealt with, as it implies a cooperation between the data sender and all the data receivers to correlate and take into account any request from the data subject. Further, in case of additions to the list of data receivers, the updated list has to be brought to the attention of the respective data subject.

---

[18] James C. Cooper, *Anonymity, Autonomy, and the Collection of Personal Data: Measuring the Privacy Impact of Google's 2012 Privacy Policy Change*, 2017, https://ssrn.com/abstract=2909148 , last accessed on 17 December 2019. George H. Pike, *Google, YouTube, Copyright, and Privacy*, 2007, https://ssrn.com/abstract=1636395 , last accessed on 17 December 2019. Ira Rubinstein & Nathan Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 2013, https://ssrn.com/abstract=2128146 , last accessed on 17 December 2019. Trautman, Lawrence J., *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks*, 2017, https://ssrn.com/abstract=3067298, last accessed on 17 December 2019 .

[19] Bert-Jaap Koops, Jasper Paul Sluijs, *Network Neutrality and Privacy According to Art. 8 ECHR*, European Journal of Law and Technology, Volume 3, No 2, 2012.

[20] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 2011, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf , last accessed on 28 February 2020.

[21] CNIL, *Guidance concerning the sharing of data with business partners*, 2018, https://www.cnil.fr/fr/transmission-des-donnees-des-partenaires-des-fins-de-prospection-electronique-quels-sont-les , last accessed on 21 December 2019.

On the transparency aspect, one matter mentioned by CNIL[22] (Commission Nationale de l'Informatique et des Libertés) was that the information notice was difficult to read and understand by individuals, due to the manner in which it was presented, but also due to lack of clarity about the data processed by the large number of services provided by Google (around 20), which combined data about users among themselves in various manners.

The decision of CNIL was mainly on the lack of proper consent obtained from individuals, as this consent was not properly informed, specific or unambiguous. Thus, the sharing of data among the various entities involved in the advertising does not have a proper legal basis under data protection legislation.

In a similar context, the Dutch data protection authority investigated the aggregation of data obtained through its various services and products (search engine, web browser, email client, video streaming, and online maps). The authority concluded that the consent obtained for the sharing of data was ambiguous and not sufficiently informed. [23] Further, the necessity for aggregation of data under the legitimate interest legal basis was not sufficiently substantiated.

Thus, this transparency aspect relates to the reasonable expectation of the data subjects about the transfer of their data based on the information they have been provided. This should be ensured for clients of private entities. However, it may be debated for data pertaining to perpetrators (potential perpetrators), as detailed in the previous section.

The purpose limitation for the data transfer should also be clearly stated in the privacy policy and in the contractual documentation concluded with the entities that receive the data. The purpose for transfer should be compatible with the purpose for which the data was initially collected. In this case, for activities of prevention of potential cyber-attacks. Thus, data may not be used for any other purpose, especially for any segmentation of clients and marketing purposes. [24]

Data sharing can take several forms, depending on the receiver of data and number of stakeholders involved, respectively, reciprocal exchange of data between two entities, entity(ies) sending data to third party(ies), several companies putting together information they hold, one-off disclosure of data to third parties.

Provided that data is anonymised when shared with third parties, it may be argued that only non-personal data is being transferred. In terms of non-personal data to be shared between companies, EU has recently adopted a regulation[25] in this respect and issued a guidance[26] for the interaction of the legislation concerning data protection and the one concerning non-personal data. The guidance includes reference to cases where there is a mixed dataset (including both personal and non-personal data), which

[22] CNIL, CNIL imposes financial penalty against Google LLC, 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc , last accessed on 3 December 2019.

[23] Dutch *Data Protection Authority, Investigation into the combining of personal data by Google, Report of Definitive Findings*, 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf , last accessed on 5 December 2019.

[24] Saberlotodo Internet, S.L. - Judgment of June 6, 2012 - Spanish National Court of Appeal, https://www.iberley.es/jurisprudencia/sentencia-administrativo-an-sala-contencioso-sec-1-rec-594-2009-06-06-2012-13777081 , last accessed on 5 December 2019.

[25] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[26] European Commission Communication, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 29 May 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2019:250:FIN&from=EN , last accessed on 5 December 2019.

usually occurs when profiling activities are also intended by the companies, including big data,[27] artificial intelligence or internet of things network. In such case, there are two approaches:

If the personal and non-personal data can be divided, GDPR is applicable for the personal data part of the dataset and the above regulation is applicable for the non-personal data.

If the personal and non-personal data are inextricably linked, data protection legislation is applicable to all data. This situation can occur if it would be impossible, technically not feasible or economically inefficient to separate the two types of data. Also, there may be cases where separation of the dataset can decrease the value of the dataset or it may be difficult to clearly differentiate between the two types of data. Nevertheless, the separation of these two types of data is not mandatory and is left as a choice of the companies holding the data.

The below requirements are analysed from the perspective of sharing data and their specifics in this scenario. As a general note, the ECJ (European Court of Justice) held that the rights of data subjects override, as a rule, the economic interests of companies.[28] However, if the data is transferred only for prevention of future attacks, this would not be included in the concept of economic interests of a company.

In case of threat data sharing, the main types of personal data found in the files shared may pertain to (i) employees, (ii) clients, (iii) individuals related to employees/clients, (iv) the perpetrator or (v) to the individual holding the IT systems used during the attack. For these categories of data subjects, it is difficult to implement the information obligation for the data processing, due to lack of proper details of the data sharing until it takes place. For the employees, client and related data subjects, a general statement may be included in the information notice they are provided with at the outset of the relation with the entity. This should reflect also a description of the data sharing system and the possibility of the data to be transferred to entities in countries that do not have an adequate level of protection of personal data. For the perpetrator, it depends on certain specifics of the situation. For instance, if the information is also sent to the criminal investigation bodies, the perpetrator should not be notified of the data that is included in the case file and the content of the case file has not to be disclosed.[29] This is relevant if the attack was successful or not. If the data is not sent to be part of a criminal file, it may be argued that the prior notification of data processing should be made to the perpetrator. In US legal doctrine, it was mentioned that entities could include a file on the desktop of the honeypot (a visible location) with the data processing details and that this is sufficient in terms of brining to the attention of the perpetrator the information notice.

For the entities receiving the data, it may prove impossible or disproportionate to provide such information notice and, consequently, they may try to invoke this exemption from the information obligation.

Thus, the transparency requirement may prove tricky in terms of bringing to the attention of the individuals whose data is being processed the data sharing activity.

[27] Sumithra, R. and Parameswari, R., Security, Privacy Issues and Challenges in Big Data and Cloud Security: A Survey (2018). International Journal of Advanced Studies of Scientific Research, Volume 3, No. 10, 2018. https://ssrn.com/abstract=3319251 , last accessed on 29 February 2020.

[28] ECJ, Case C131/12, Google.

[29] Stephanie von Maltzan, No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System, European Journal of Law and Technology, volume 10, No 1, 2019.

Legal basis for transfer

There are a number of types of legal basis for sharing data mentioned under data protection legislation. For the sharing of data mentioned in this section, the below potential legal basis are analysed, in order to identify whether there was a right for the access and transfer of data. This impacts on the criminal law angles. In the case of intermediaries, legitimate interest and consent are frequently used. The applicability of the main types of legal basis are analysed in the following sections.

Legal obligation: The legal obligation may relate to the sender of the data or to the receiver of the data. This is a situation in which it is clear which data and to whom it has to be sent. This legal basis is complemented by the legitimate interest in cases where there is a general legal obligation (e.g. to perform reporting to an authority in a centralised manner for a group of companies), if the data to be processed for the reporting and the need to transfer such data to the other members of the group is not expressly mentioned under the legislation. In this case, it depends on the interpretation of ensuring state of the art security measures and notification of security incidents. However, as these two legal obligations are rather general, further clarification is required in order to consider this legal basis applicable for all data sharing situations detailed above. Currently, for any data transfer not covered by the legal obligation, the legitimate interest analysis is performed prior to data sharing.

Legitimate interest:[30] The legitimate interest may pertain to the data sender or to the data receiver. However, this has to not have negative consequences on the data subject's rights and liberties. One interesting case involving the sharing of data between the members of a gas station association in Sweden[31] involved the sharing of CCTV of vehicles that left the gas station without paying. The aim was to prevent future similar actions of the identified vehicles in gas stations. This approach was considered excessive by the Sweden data protection authority due to the large scale processing and creation of blacklists. Interpretation of the applicability of the legitimate interest as a legal basis for processing, as it has to be assessed on a case by case basis. Legitimate interest with the intent to ensure prevention of systemic attacks in a particular sector and, thus, comply with proper security measures in order to face existing attacks.

Consent: Consent obtained for data sharing has to fulfil (as in other cases when consent is needed) certain conditions. German courts have mentioned that it is "the authority of the individual to decide for himself, on the basis of the idea of self-determination"[32]. The consent would be difficult to implement as legal basis. For data pertaining to clients, this entails the deletion of data once the consent is withdrawn (from the IT systems of the private entity that collected the data and from the IT systems of the subsequent receivers of personal data). Further, a mechanisms for managing consent has to be implemented. For data pertaining to the perpetrator, this legal basis is not practical in terms of obtaining the consent and ensuring withdrawal thereof.

Public interest: It may be argued to some extent, that, as NIS Directive includes the basis for sharing of data on types of attacks, it can be a basis for sharing of minimum personal data related to such attacks in order to ensure the public interest covered by this directive.

Relevant for the legal basis for sharing data are cases when data is collected for one purpose and transferred for another (subsequent) purpose. In such cases, a compatibility test had to be performed between the initial and subsequent purposes. The purpose of the processing should match or be similar

[30] ECJ, C-13/16, Rigas on the interpretation of the legitimate interest concept.

[31] Nymity, *Deciphering legitimate interests under the GDPR*, https://info.nymity.com/deciphering-legitimate-interests-under-the-gdpr , page 24, last accessed on 5 December 2019.

[32] German Constitutional Court, BVerfGe 65,1; 1983.

to the purpose for which the data had been collected. This ties in with the reasonable expectation of individuals in terms of the processing of their data. Such aspects have been detailed by Working Party Article 29 in the context of behavioural advertising[33] and in relation to purpose limitation.[34]

Thus, any processing following collection should be checked for the purpose compatibility test.[35] A different purpose does not necessarily entail that it is incompatible to the initial purpose.

The compatibility test focuses on the following points:

- Similarity between the initial purpose and subsequent purpose.
- Reasonable expectation of the individual with respect to the subsequent purpose. This depends on the first point on similarity of purposes and on the information that was provided to the individual at collection time.
- The types of data processed and the consequences of the subsequent purpose on the individual needed are similar to the initial purpose.

Further, the compatibility test is performed on a case by case basis. Therefore, for each type of data sharing, if other legal basis is not applicable, the compatibility test has to be performed for each type of personal data shared.

The usual example given in this respect is the improvement of a mobile application. The subsequent purpose helps in the service provisioning that represents the initial purpose. Individuals are expecting that the mobile application will be improved from a technical and functionality perspective. This can be supported further by an information provided to individuals about such processing for data actually needed for technical and functionality improvements. This is applicable if the data processed is limited to the data needed for the technical and functionality improvements (there are some examples in the below sections in which more data than needed is transferred).[36] Data processed for this subsequent purpose impacts only the technical improvements of the mobile application, without any impact on the type of service or manner of providing the service to the individual.

An example of data used for subsequent purposes is mentioned in a decision concerning a medical clinic that collected the email address of individual with the purpose of establishing appointments and making surveys about the satisfaction of the individuals with the medical services provided by the medical clinic. The medical clinic subsequently used the email addresses to send commercial communication (containing various offers of medical services) to the individuals. In this case, the court clearly stated that such subsequent use of the data is not in compliance with the initial purpose for collecting the data and is not in compliance with data protection legislation (as it also required the consent of the individual for receiving marketing materials).

The public interest legal basis and vital interest legal basis may also be considered. However, there applicability is rather narrow.

---

[33] Working Party Article 29, *Opinion 2/2010 on online behavioural advertising*, 2010.

[34] Working Party Article 29, *Opinion 3/2013 on purpose limitation*, 2013.

[35] Sabah S. Al-Fedaghi, *Beyond purpose-based privacy access control*, ADC '07 Proceedings of the eighteenth conference on Australasian database - Volume 63, Pages 23-32.

[36] ENISA. 2013. Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs. (Oct. 2013). https://www.enisa.europa.eu/activities/cert/support/information-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport , last accessed on 28 February 2020. Václav Stupka et al., Protection of personal data in security alert sharing platforms, 2017, https://dl.acm.org/doi/10.1145/3098954.3105822 , last accessed on 28 February 2020.

The legal basis has to also be analysed in case of transfer of data to a country without an adequate level of protection of personal data. This may occur in case of aggregation of data by a private entity at a global level or in case potential threat information is posted on a publicly accessible website.[37] In such cases, personal data may be transferred if it is expressly required for public interest or vital interest purposes. In addition, the transfer can occur in case standard model clauses are signed between the entities that participate in the data sharing exercise.

Data minimisation principle

This legal requirement translates into the following three aspects that should be taken into account.

Only data needed for the processing purpose should be collected and processed, with no excessive data being collected, stored or processed[38]. This depends on the specificity of the purpose for processing or sharing data. Thus, only data needed for the processing should be collected. Further, if data has already been collected and is being stored, for subsequent processing[39] or new iterations of the initial processing a verification has to be performed before the data processing or data sharing takes place in terms of the amount of data to be shared. One example in the case law of the ECJ[40] refers to metadata collected about individuals. In this decision, the excessiveness of data collected for the purpose of providing a calling service, such as metadata on date, time, duration and type of a communication, identification of communication equipment and location thereof, the number called and an IP address for internet services, as such information could provide a very detailed profile about an individual.[41]

Data protection aspects and especially data minimisation is relevant also in case of BYOD models, as, in such cases, generally, it may be argued that only the data pertaining to the work container can be extracted without the consent of the employee at the moment of extraction, as the internal policies and procedures generally provide for such situations from the outset.

One needs to analyse whether using aggregate data is sufficient for the purpose of the attack data modelling and threat prevention. In certain situations, the aggregation would lose the granularity that the data modelling requires. In other situations, there is a need to be able to revert to the individuals whose data was profiled in order to be able to prevent attacks and understand if multiple types of attacks are used by a particular perpetrator and, thus, the aggregation brings issues in achieving this purpose.[42]

The data minimisation requirement is linked to the limitation of entities/individuals having access to the data and to the period for which such access is granted. Thus, it should be analysed in each case of data sharing. This ties in with the requirement of any stakeholder (which should include intermediaries) to limit access to the personal data on a need to know basis. In cases where data is stored

[37] Cedric M.J. Ryngaert and Nico A.N.M. van Eijk, *International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees*, International Data Privacy Law, Volume 9, No. 1, 2019.

[38] Wright, D., & Raab, C., *Privacy principles, risks and harms*, 2014, International Review of Law, Computers & Technology, 28(3), 277–298.

[39] ECHR, Gardel vs. France, para 62, concerning the inadequate use of data.

[40] ECJ, Cases C293/12 and C594/12, Digital Rights Ireland, 2014.

[41] Michael Barbaro & Tom Zeller, *A Face Is Exposed for AOL Searcher No. 4417749*, NY TIMES, Aug. 9, 2006 details how anonymised search logs can be used to re-identify individuals. Christopher Kuner, *European Data Privacy Law and online business*, 2nd Ed. Oxford University Press 2007, page 91-95 – IP personal data

[42] Kaltheuner, F. and Bietti, E., *Data is power: Towards additional guidance on profiling and automated decision making in the GDPR*, IRP&P.

by the intermediaries for their users, one may argue that the obligation is applicable for the users and not the intermediary. In this respect, further legal clarification on the level of support the intermediaries should give to users for setting-up a default level of access management and, implicitly, security of data.

In practice, entities use third parties to set up the communication system for threats or potential threats. As mentioned above, the need to know principle can be implemented through a centralised system that stores all data shared between the parties. If the transfer is not performed through a centralised system, it would be much more difficult to manage from a regulatory perspective. Thus, a centralised system would be preferred. Examples of sharing formats on the market include STIX and TAXII.[43]

For the centralised system, if algorithms are in place in order to identify patterns of attacks or correlation between multiple attacks, the algorithm has to be analysed form a data protection perspective. If automated decisions are taken based on the outcome of applying this algorithm, the specific requirements on automatic decisions have to be implemented.

The establishment of limitation of data sharing can also take into account (especially in terms of legitimate interest)[44] the number of individuals potentially affected by the data sharing, the number of individuals potentially affected by the identified security incident, percentage of IT system having the particular vulnerability, level of impact of the vulnerability use, including economical.

The centralised system should be created with rules for deletion of data that becomes irrelevant or that does not need to be in the system. Further, when participants retire from the system, the data they send can be either deleted or not, depending on the legal basis for transfer and the data they received can be deleted or not, depending on the legal basis.

Mechanisms for new participants (and history of data they can see), making sure that perpetrators (whose data might be stored in the system) do not become participants themselves. If no mechanism is in place to prevent such abuses by participants, the participants can be considered accomplices to the perpetrator.

A framework for handling data subject requests and deletion of data should be established. Further, the receivers of data should inform the other participants of any data breach on their side concerning the data obtained from other participants. Each participant should be obliged through the participation agreement not to use the data for active defence mechanisms that are illegal.

Aggregation is performed also by network companies through the metadata obtained from multiple clients from all over the world. In this case, there are two levels of agreements to be set in place: one between the entities from which the data is collected and the network companies and one between[45] the network companies and the recipients of the data. For this data transfer the network company becomes data controller and it is liable for all of the matters mentioned above. It has to manage the participants in terms of data access.

[43] ENISA, Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers, December 2016, https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/at_download/fullReport , last accessed on 8 March 2020.

[44] Cf. Céline van Waesberge and Stéphanie De Smedt, Cybersecurity and Data Breach Notification Obligations under the Current and Future Legislative Framework, 2016, EDPL .

[45] ENISA, Incident Notification for DSPs in the Context of the NIS Directive, https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/at_download/fullReport , last accessed on 8 March 2020.

The use of centralised SIEM (security information and event management) systems with data sharing between private entities[46] may be considered excessive, as a significant amount of data is not relevant for threat prevention, as it represents day-to-day activity of the private companies. Thus, in terms of legal basis for data processing, this cannot be substantiated, as it does not fall under a legal requirement and the interests of the private companies do not surpass the rights of the data subjects whose data is aggregated, profiled and shared with a large amount of entities. This type of data sharing is likely to be considered intrusive by the data subjects. As a result, if a SIEM centralised system is used by multiple private entities, the data of each entity has to be kept separately.

Of course, in terms of current legislation, the data sharing for significant security incidents is generally defined from private entities to public authorities and between public authorities. Unfortunately, even for these scenarios, there is no guidance on the types of personal data actually needed for the data processing purpose. Further guidance is needed and can be created on a scenario based approach, depending on the type of attack. Further, the NIS Directive applies only to certain sectors and to certain private entities within those sectors.

The transfer of data concerning threats and potential threats may be made to third parties that are private entities, including entities within the same group of companies, to private organisations and to entities that have set-up the security operation centre, that operate the SIEM (security information and event management) or that centralise the security incident data. These may include transfer of confidential data, that, as per legal requirements, either should not have been in the possession of the sender or that should not be disclosed by the sender.

Other legal implications of data transfers

In relation to the data pertaining to the perpetrator, this action may involve transfer of data without a right. In this case, the criminal offence of transfer of data obtained without a right may be applicable.[47]

Further, violation of private life may also be applicable for private data obtained without a right and for transfer of such data to third parties

Access to beacons or to malware found in the files copied by the perpetration should not be given to other private entities, as this would constitute, aside from the criminal angles mentioned above, breach of other legal provisions in terms of surveillance.

The transfer of any data that was obtained illegally by the victim, by perpetrating the criminal offences related to entrance, change or disturbance of the IT system of the perpetrator (or other IT systems involved in the attack) constitutes in itself a criminal offence. Further, the setting-up of a system by private entities in a specific sector to share such information among them constitutes a criminal offence perpetrated by all members of the system, irrespective if they shared or not data, as they are accomplices to any criminal offence perpetrated in this respect.

[46] Stephanie von Maltzan, No contradicton between Cyber-Security and Data
Protecton? Designing a Data Protecton compliant Incident Response System, European Journal of Law and Technology, volume10, Issue 1, 2019.

[47] Irish Data Protection Commissioner, Data Sharing in the Public Sector, 2019. Gina Fisk et al., Privacy Principles for Sharing Cyber Security Data, 2015 IEEE Security and Privacy Workshops, https://ieeexplore.ieee.org/document/7163225 , last accessed on 28 February 2020.

Data in the files that were copied by the perpetrator (for instance, data used by a private entity to find them on Darknet), should not be given to any private entities (aside from a service provider that actively searches on behalf of the victim for these on Darknet), as this would constitute breaches in terms of data protection and criminal offences related to professional information.

2. Handling whistleblowing related to data security

In 2019, the EU has adopted a Directive[48] outlining principles for companies to set up whistleblowing hotlines and specific policies and procedures related to collecting information about potential breaches of the company of EU law in specific sectors (including protection of privacy and personal data, and security of network and information systems), together with procedures for investigating these and for protecting the whistleblower from any negative consequences.

We are outlining in this section the main points to consider when setting-up such hotline, as outlines in the Directive. For each specific country in the EU, further details may be provided in national legislation implementing the Directive. This type of hotline is also relevant in the context of offensive security, as, it may be the case that either employees of the company or service providers performing the offensive security exercise may wish to bring to the attention of the company certain aspects through this hotline.

The Directive is applicable for whistleblowers that are employees of a company or not, as detailed in article 4 of the Directive. The main takeaway in this section is that individuals working on behalf of the offensive security provider may also qualify as whistleblowers under this Directive. In addition, the persons to be subject to protection in the context of whistleblowing (especially against any retaliation) includes the whistleblowers themselves and, among others, the companies these work for.

The Directive covers the reporting of breaches of EU legislation. In terms of level of knowledge of a breach or a potential beach, the Directive mentions 'information on breaches' to mean "information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches".[49]

Companies, as per the Directive, have to establish internal and external communication channels (hotlines) which includes anonymous reporting, together with mechanisms for analysis, including the following steps:

- Designation of impartial person/department for receiving information.
- Record keeping of the exact information received – e.g. recording of conversation, saving of emails.
- Establishment of an impartial team to investigate any allegations in a diligent manner.
- A reasonable timeframe for resolving the allegation and timely feedback on the progress of the investigation.
- The company to ensure confidentiality about the identity of the whistleblower during the investigation and afterwards, except for any legal obligations to make such disclosure, like disclosure to authorities or courts of law.

[48] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

[49] Please see Article 5 of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

In certain circumstances outlined under the Directive (such as, prior disclosure to internal hotline without a proper response or imminent danger to public interest), public disclosure of information about breaches can fall under the Directive and ensure protection for the whistleblower.

Any disclosure in such circumstances relating to IT security is essential and it is recommended to analyse any vulnerability identified and disclosed through the hotline as soon as possible in order to avoid third parties or public disclosure of such vulnerabilities.

The company should not allow for retaliation to occur, including aspects such as suspension, dismissal, harm (including any reputation damage), discrimination. Further examples are included in Article 19 of the Directive.