# Data protection and legal aspects in the context of red team and penetration testing activities

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Services related to offensive security involve access of third parties to the architecture of the network/applications of the company and also to data (personal data, confidential data, trade secrets). This entails the need to ensure proper steps and procedures are followed when handling such data, in order to prevent any negative consequences on the operations of the company. In such cases, as the services providers have access to the data usually handled by company employees, it is recommended to reflect best practices in terms of confidential/personal data handling in such interaction. Thus, such service providers have access to the internal IT systems of the company similarly to employees working on/with those IT systems and, consequently, measures similar to those imposed on employees are recommended to be reflected in the relation with the service providers. This entails the need to focus on preventive measures and ensure contractual documentation allows for remedial measures to be taken by the company.

A risk assessment of the planned actions for the offensive security exercise, reveals the sensitive areas or assets for which the company might decide to have contractual provisions.

For this reason, it is recommended to analyse at the outset the actions taken by a company internally or through external service providers in terms of offensive security from a data protection and legal perspective. Depending on the type of actions taken and the manner of implementation, specific aspects can be contemplated to be included in the implementation and/or specific clauses can be included in the agreement with the service providers. The purpose of such clauses is to set out the landscape for the exercise and act as a basis for the training made to individuals on the assignment.

Generally, such contractual provisions are useful to provide clarity on actions to be taken by each entity in cases where a data breach occurs, either in a voluntary or involuntary manner or in cases when a security incident occurs on an IT system on which penetration testing occurred.

This section first provides insight into the scope of offensive security service agreements, including practical suggestions on how to structure the scope and correlation with the other clauses in the agreement, especially from a liability and confidentiality obligation perspective.

Subsequently, we detail the data protection and confidentiality practical points to be analysed and reflected in the agreement and/or implementation. These are sensitive aspects, as it is advisable for these to reflect legal requirements and also are closely linked to the business operations. The use of third party tools is also analysed from these perspectives.

The scope and the confidentiality clauses reflect also important point in terms of establishing the limitations of the exercise and to provide awareness of consequences in case of going beyond these limits or not fulfilling requirements properly. These situations and implications are detailed as well, together with conditions for liability in order to emphasise the usefulness of including clear contractual provisions from the outset and enforcing such contractual provisions throughout the exercise, including through training of employees of the parties.

Throughout the section, we reference penetration agreements, but the matters can be applied also for red teaming agreements, provided that they are relevant for the scope of the red teaming agreement.

The below analysis points and recommendations relate to preventive steps to be taken in terms of compliance, data protection and security of data, but also remedial steps in case of breach of contractual obligations or tort liability.

## 1. Scope of offensive security agreements

The scope of the penetration test or red team exercise has to be established before its start and can be changed subsequently (for the performance of a subsequent penetration test), when unanticipated use cases/aspects become relevant. In terms of red team exercise, the scoping might be more general, referring to the purpose/end result, rather than detailed - as is the case of penetration testing. The below points referring to penetration testing are also relevant for red team exercise.

The scope is set through a risk based approach performed by the company or together by the company and the penetration testers. The analysis can be based on importance of the IT system in the ecosystem of the company. Also, the risk analysis has to be aligned to the expectance of threats on such IT systems based on the current threat landscape. Thus, the scope can be determined together by the company and the service provider providing the penetration testing services. In case of penetration testing, the analysis can be performed based on internal risk assessment methodologies, service provider methodologies or legal requirements that have to be monitored continuously. This approach is not applicable in case of red team exercises, as these are focused more on the goal of the exercise, leaving the methodologies choices up to the red team.

The scope of the penetration testing has to also be defined by reference to the type of IT system being analysed. Thus, the penetration testing can focus on the software (mobile application, web application, server and client side, together with any related middleware), on the network of the company (or part of the network) or implementation of the infrastructure (including servers, operating systems and firmware on hardware.

Further, the scope of work can include the methodology to be used for the testing phase and for the threat rating. On the one hand, this is relevant in order to ensure that all the aspects that have been agreed to be tested are covered in the testing exercise. On the other hand, this is relevant in order to ensure that all legal obligations concerning IT system testing are covered (including use cases, threat testing, legal obligations directly incumbent on the company or indirectly, when the company provides services for other entities subject to such legal requirements). This is applicable for certain sectors having specific legislation in terms of security of IT assets.

The specification of scope for penetration testing or for red teaming is relevant in defining the limits of the IT system accessing, and for protecting both parties when access without a right has to be determined. This aspect is described below in section 3, together with the proof of concept.

Such scoping exercise is relevant also in cases where penetration testing reports are used by auditors in their assessment of the IT system.

In terms of penetration testing lifecycle, it is advisable to consider from the outset if the service provider will perform any re-testing after certain findings are mitigated in order to include it in the penetration agreement. Alternatively, the re-testing can be performed by another service provider.

From a contractual perspective, there are two approaches that can be taken: either a single agreement reflects all aspects of the penetration service exercise (including confidentiality/non-disclosure aspects, commercial points, scope of work), which is usually used for one-off assignments, or a master services agreement is concluded with the service provider (containing confidentiality/non-disclosure aspects, some commercial points), whereas the scope of work and certain commercial points are included in statement of works for each individual penetration testing exercise.

Thus, in order for the scope of work to be clear for and binding on both parties (the company and the service provider), it is recommended for it to be included in the penetration services agreement/statement of work, in purchase orders or circulated through the manner of communication established between the parties for sending instructions.

In terms of obligations being binding on the service provider, it is recommended to have all essential requirements included in a document signed by both parties or mentioned in the agreement as being binding in terms of obligations. Generally, if specific requirements are mentioned in the RFP phase (e.g. number of certified persons performing the testing), in order for these to be legally clear for the parties, it is recommended to include them in the contractual documentation as well. This ensures an easy to follow framework for the service provision, making it easier for any member of the team working on the exercise to know the overall aim of the exercise and the steps to be followed. Usually agreements mention that they supersede any prior agreements and information provided in RFP phase is not an obligation of the service provider to act in a certain manner.

## 2. The concept of personal data in offensive security

Personal data represents data that can lead to the identification of an individual or makes an individual identifiable when correlated with other data available to the entity trying to identify the individual. Thus, in an organisation environment, this includes data and any pseudonymised data in IT systems. As testing and development environments (by applying the data minimisation and need to know principles) generally should not hold production data, these environment should contain anonymised or synthetic data. This is an implementation of the minimisation principle and of the need to know principle. On the one hand, only personal data specifically needed for a data processing purpose should be used. In this case, generally as long as the IT systems and IT architecture is similar to the production one, actual production data is not needed. Only persons that need to have access to personal data should have access to it. In this case, in most cases, access to actual personal data is not needed, as the interest is to test the various technical and organisational aspects of the IT infrastructure and IT systems.

However, the protection of personal data has to be viewed in context. Even if the red team exercise or penetration test is performed on testing environments or on production environments for a limited period of time, the protection of personal data has to be ensured also for the future. Vulnerabilities identified in testing environments exist also on production. Thus, offensive security exercises also contribute to a higher level of protection of personal data.

In terms of specifics concerning of protection of personal data, offensive security exercises should take into account the following. Depending on the specifics of the exercise, certain steps can be taken in terms of the below points. For the red team exercises, the main aspects to be agreed with the service provider are the location of data extracted from the IT systems and general processing during and upon completion of the red team exercise for the data extracted/collected by the red team, whereas the blue team has to ensure security measures are in place in the company IT infrastructure.

- **Accessing data:** The amount of data and types of data to be accessed by the service provider are to be assessed on a case by case basis and they are to be closely correlated with the scope of the agreement. Section 3 below outlines several steps for protection of confidential data that can be applied also for access to personal data.
- **Transfer of data:** Any transfer of data has to be analysed in terms of compliance with legal requirements. This is especially necessary when data is transferred to servers pertaining to the service provider or to third parties. In case of public cloud storage, data protection analysis has to be made in terms of the cloud service provider.

- **Scope of data processing:** The data processing scope should reflect the data processing activities performed in order to fulfil the scope of the offensive security agreement. This entails the identification of each type of data processing activities and the types of personal data that need to be processed. Section 3 below outlines several steps for protection of confidential data that can be applied also for protection of personal data in terms of scope of processing and data minimisation of data disclosed.
- **Sub-contractors:** Sub-contractors of the offensive security service provider are most likely data processors under the data protection legislation. When sub-contractors are used, it is recommended for the company to identify which obligations from the service agreement should be replicated in agreements with sub-contractors. Emphasis is placed on transfer of data, confidentiality requirements and limitation of liability. Use of open-source solutions is useful from a practical and cost perspective. However, in such cases, an analysis has to be made on where data is stored and transferred.
- **Data retention:** The data collected during the offensive security exercise is to be held by the offensive security service provider and the company only for the amount of time needed. For example, the service provider should hold the personal data only until it delivers the report to the company, while, afterwards, it should pseudonymise the data (if it is needed to prove the performance of the agreement), delete it or anonymise it (if it not needed for other purposes). In turn, the company can decide to hold the personal data, for instance, only until it identifies how to remedy the vulnerability identified in the offensive security exercise.
- **Security details:** In order to prioritise their implementation in accordance with legal requirements, the specific security technical and organisational matters can be implemented on a risk based approach and taking into account the level of access of the service provider, the type of personal data which it has access to and the location for storing data during the performance of the exercise.
- **Anonymisation/psedonymisation:** In certain instances of penetration testing or of red team testing anonymised or pseudonymised data can be used. This is the case when production-like environments are used for the exercise. As a simplified definition, anonymised data entails that no individual can be identified or identifiable from the anonymised data, whereas pseudonymised data entails that an individual cannot be identified or identifiable without additional data kept separately from the pseudonymised data.
- **Data breach notification:** A process should be established for notifying the company in case of data breach occurring on the side of the service provider or its sub-contractors. A data breach can occur in the context of a penetration testing in case the actions taken by the penetration testers lead to loss of confidentiality, integrity or availability of personal data that was not in the scope of the penetration agreement. For example, if data is accidentally exposed to the public or if a service becomes unavailable to customers of the company because of actions taken by the penetration testers. Alternatively, identification of a data breach may also be relevant when a penetration tester identifies an already existing data breach in the IT systems of the company. This type of obligation is to be cascaded throughout the supply chain and should also take into consideration any other legislation concerning data breach notification.

The above aspects can be detailed in a data processing agreement concluded with the service provider. Generally, the service provider can be qualified as a data processor and, in such situations, the conclusion of a data processing agreement is mandatory. In case of sub-contractors being used, the service provider should undertake to replicate its obligations under the data processing agreement in any agreement with its sub-contractors.

## 3. Practical aspects concerning confidentiality obligations and conflicts of interest

In terms of protection of company know how and confidential information, there are several legal aspects that have to be included in the penetration agreement.

Trade secrets are defined by law[1] as information that satisfies all of the following conditions:

- it is a secret that is not known among the circles that normally deal with this kind of information;
- it has commercial value because it is a secret; and
- the company took reasonable steps given the specific circumstances to keep it secret.

Whereas the knowledge of certain information among professionals in a specific sector or known to the public can be determined to some extent, the commercial value of such information may be difficult to prove by a company. This entails proving a directly or indirectly liaison between the secrecy of information and the product/service sold by the company.

The first step in order to ensure protection of trade secrets is to have a confidentiality agreement in the offensive security agreement in this respect. This agreement can only cover the information that fulfils all of the above conditions cumulatively. In order to reflect legal requirements, it is recommended for the clause to include at least the following aspects:

- the types of information that is confidential, for instance, any information provided throughout the performance of the agreement.

- the situations in which confidential information may be provided to the service provider, such as, instructions, written documentation, oral presentations, during the performance of the agreement when accessing the company IT systems.

- the exclusions from the confidentiality agreement, such as data publicly available, data obtained through other sources, data developed independently, data already known by the service provider. The exclusion concerning information already known publicly or in certain circles of professionals stems from the legal provision outlining the conditions of trade secret qualification.

- the disclosure right, which includes situations in which confidential data may be disclosed to third parties. This generally covers situations of legal obligations, such as disclosure to auditors, authorities or courts of law.

- details of the persons to whom the confidentiality obligation applies, which may include the service provider and all employees of the service provider. For the latter, a commitment can be undertaken by the service provider to ensure that its employees comply with this requirement and specific training on this can be made.

The confidentiality agreement is generally applicable for intentional disclosure of confidential data. In case of unintentional disclosure, the liability clause becomes applicable.

In terms of timing, in order to produce effects, the confidentiality agreement should be signed prior to any confidential information is disclosed to the service provider. In certain situations, this entails that it should be signed during the request for proposals phase, as, in this phase, by asking questions

[1] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

about specific infrastructure products and configurations, confidential information about the company IT systems are disclosed.

Among the situations in which trade secrets are lawfully obtained is the observation, study, disassembly or testing of a product that has been made available to the public. It could be argued that, in this case, the offensive security testers testing a web application or mobile application have rights to use any such results of their analysis. Of course, this can be argued for any black-box situation, as in grey-box or white-box scenarios, they have access to more information than what is only made available to the public. In order to avoid such situations, the agreement for the services provided can include a limitation on using any information resulting from the activity performed under the offensive security agreement.

Thus, as mentioned above, in order to be able to protect trade secrets, the company has to ensure that it mentioned expressly what constitutes trade secrets (confidential data) and has to take active steps in protecting the unauthorised disclosure of such trade secrets. In case there are sub-contractors involved in the services provided, the company has to ensure all such sub-contractors make the same guarantees and undertake the same obligations as the service provider.

The condition of active steps taken by the company entails that these have to be properly documented and may include, aside from the contractual clauses mentioned above, technical and organisational steps, including the examples below.

Active steps in this context can be established on a case by case basis, depending on the medium on which the confidential information is stored, the manner in which it is communicated to the service provider and the instructions received by the service provider at the outset of the service provision and throughout the service provision:

- **Reiteration of confidentiality:** Reiterate the confidentiality level of document/information in writing or verbally when the document/information is provided.
- **Access limitation:** The service provider can use of enterprise computers with enterprise **accounts**. Alternatively, the service provider uses a VPN connection for certain tests, when possible. Access is limited based on the scope of the testing exercise and alerts should be triggered when the scope is exceeded. Further, the testing should end when a proof of concept is completed, without the need to go further than that with data exfiltration, for instance. For red team exercises, as it entails creative means of entering the IT systems and extraction of data and, consequently, not a play-by-play establishment of the tests performed during the exercise, the access management mentioned above is usually not applicable in this case. Further, it is important for the company not to forget to remove access once the penetration test is completed. Even in cases when the same service provider is used for re-testing or for other penetration testing exercises.
- **Logging:** It is recommended for the exercise to be covered by logging both on the side of the company and of the service provider. This is useful in order to determine the facts when there are queries in this respect from either party.
- **Real-time monitoring:** The real-time monitoring is useful in case the internal team of the company is aware of the testing exercise in order to identify any situation in which the scope of the exercise is exceeded. In such cases, time is of the essence.
- **Verification of deletion of data:** At the end of the testing process, as per the retention period and deletion obligation under data protection legislation, all data should be deleted from the IT systems of the service provider. A statement from the service provider in this respect can be obtained (including reference to deletion of all copies of data from any storage) to ensure the process was completed successfully.

- **Integrity check:** For certain situations, such as storage spaces, web application source code, integrity checks can be performed after the exercise is completed in order to ensure that these have not been changed during the exercise.
- **Vulnerabilities/incidents identified:** Contractual obligations can provide that, during the exercise, if vulnerabilities outside of the scope of work or prior security breaches (that took place on the IT systems) are identified by the service provider, these should be notified to the company. Further, any such details should fall under the confidential data definition and prohibition of disclosure to third parties, the press or third parties should exist.

The relevant controls can be put in place on a case by case basis, depending on the specifics of the organisation and on the type of confidential data disclosed to the service provider. For instance, in case of red team exercises, some of the above may not be feasible in practice due to the nature of the exercise.

The main idea that should be found throughout the confidentiality agreement/clauses is for the service parties to mention the scope of data needed for the exercise and, consequently, for the provider to have an idea of the type of data it needs to complete the exercise. In this manner, it is ensured that the provider obtains only the data needed for the performance of the service agreement and not to use the data for any personal/commercial purposes of the service provider, its employees or of third parties. This entails that the service provider guarantees that it trained its employees and has controls in place to prevent any breach of the obligations undertaken by the service provider in the agreement.

Confidentiality should also be analysed in terms of the destination of the data. For instance, when a cloud solution is used for the tests, company data may be transferred in the cloud storage for that particular tool. In this scenario, analysis should be made on the appropriateness to share the data to this third party and on assurance that data is deleted after the testing is completed. Further, in case the service provider uses machine learning tools for conducting its testing, service provider has to ensure that no confidential information is included in the machine learning tools.

In terms of using tools for which the service provider has license or other rights of use or use of third party tools, the service provider has to guarantee on the one hand that it has the right to use the tool for the offensive security exercise and, on the other hand, that confidential data (including personal data) is not transferred or stored in such tools. Or, if data is stored, it is deleted appropriately at the completion of the exercise.

Additional aspects relate to the confidentiality of the offensive security report. Generally, a company would like to use this report as basis for auditors to perform their report, in case of litigation, queries from authorities, for required notifications to authorities and for requests from clients. Of course, for each of these instances, before the penetration testing report is issued, the company has to identify the future disclosure needs for such report. In case the red team also provides a report on specific vulnerabilities it identified, the same is applicable.

In certain cases, clients of the company may request to review the content of the penetration testing. This is the case especially when the company provides IT services to its clients, such as cloud services, any hosting services or web application hosting services. In certain cases, the clients might request the penetration testing, as they have legal obligations in terms of security assessments and/or performance of penetration testing for the entire IT system it uses.

The use of reports for other purposes than internal review may be subject to additional restrictions imposed by the service provider. Generally, service providers allow for disclosure of their report to auditors, authorities or potential purchasers of the company, but they do not provide reliance on the report. Thus, third parties can become aware of the report, but they cannot rely on the report and, consequently, the service provider is not liable towards these third parties for the content of their report or the manner in which they conducted the exercise.

There are certain situations in which the company might need to prove level of security and/or the fact that it makes regular penetration tests on the IT systems it uses or on the IT systems that are integrated with its products (e.g. cloud services uses for storing certain data within the application flow).

Generally, the service provider provides a partial/truncated version of the report in certain situations. This approach is taken because on the one hand, as per legal requirements, certain details of identified vulnerabilities should be known by a limited number of individuals (based on the need to know basis) and, on the other hand, that disclosing such sensitive information to third parties (e.g. potential clients in the RFP process, to the public on its website) may lead to exploiting the unresolved vulnerabilities or use of resolved vulnerabilities as a starting point for attacks (as part of the reconnaissance process).

Thus, in such cases, a general description of the identified vulnerability together with risk rating should be sufficient, provided there are no specific legal requirements for additional details.

In terms of reproducing the penetration report, as this is protected by copyright held by the penetration service provider, a specific right to reproduce it in other documents or publications is required. This applies also when reproducing parts of the report on its website or towards authorities/third parties.

Concerning the limiting of conflict of interest, it should be avoided for an individual that previously worked for the company or was involved as external provider in the development of IT systems or auditing activities to participate in offensive security testing.

Further situations of potential conflict of interest that may lead to inefficiency in service provision or suspicion of this by authorities and third parties involve not using the penetration service provider also for SOC or auditing services. This ties in also with regulatory prohibition in specific legislation, such as the auditing legislation.

One additional point to consider in relation to confidentiality and also liability is the performance of penetration testing exercises on software/infrastructure of third parties (e.g. vendors of the company whose application is used by the company and is integrated with the company's IT systems, cloud services used by the company for storage or in another form – IaaS, PaaS). In such cases, the company does not have the right to approve a penetration test on the systems it uses. The license for use does not cover such types of uses. This is mainly because such types of services are used by multiple clients and the availability level for all clients has to remain within the agreed levels. A penetration test might lead to perturbation of the activities for other clients than the company.

Additionally, such penetration testing might lead to accessing of confidential information pertaining to the service provider or to other clients. This leads to the breach of agreements between the company and the service provider or between the service provider and the other clients.

In cases where testing of infrastructure/software pertaining to other entities is needed, prior discussions and approvals from the third party with respect to the scope of the agreement and the confidentiality of the information uncovered is needed.

Certain service providers have anticipated this needed of their clients (e.g. cloud service providers) and have provided on their website a notification mechanism for intention to perform penetration tests on their infrastructure. After a notification is submitted outlining the exact parameters for the penetration test, this is analysed and approved/rejected by the service provider. This analysis is needed in order for the service provider to have an overview of the tests to be performed and ensure that these cannot damage/obtain unnecessary access to its IT systems. This approval mechanism can be detailed in the service agreement, depending on the needs of the company, and certain use cases can be provided from the outset.

Lack of an agreement between the company and the service provider concerning penetration tests or not respecting such understanding can lead to liability of the company or of the penetration testing service provider, as detailed in the following sections.

## 4. Prevention of potential consequences in offensive security

There are certain legal aspects that should be taken into consideration when access to IT systems is involved. In this section we outline some of these potential consequences with the aim of the readers to implement prevention mechanisms, including training, in order to avoid such types of consequences. The below represent a wide range examples of potential situations that can occur, with the actual potential consequences depending on a case by case basis. It is worth noting that, in most cases detailed below, intent is a requirement for legal implications for the individual performing the action. Negligence generally does not lead to such legal implications.

Further, the below is aimed at providing awareness about legal implications of specific actions that may take place in the context of professional services provision, first describing certain legal concepts and the conditions that have to be fulfilled in order for these to become applicable.

Actions taken by service providers outside of the agreed scope of work may lead to certain consequences in accordance with legislation, including criminal law implications. As mentioned, in this section, we outline the main points to take into consideration, together with practical aspects in order to prevent any perpetration of criminal offences and criminal law liability during offensive security testing. The section focuses on the provisions of the Budapest Cybercrime Convention of 2001 and, as an example, on the Romanian Criminal Code. As countries generally have independent decision power in terms of the criminal law they adopt at the national level, such provisions may differ slightly from country to country, even if they implement the same international convention.

The first important concept to be clarified in this context is the IT system concept. The Budapest Cybercrime Convention defines IT systems as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.[2] Case law has extended the concept of IT systems in order to cover any types of software, web application, database, microservices, computer, API, email server, etc.

The IT system access can be analysed at different levels, depending on the method of accessing: can be located at the back-end application level (lack of SQL injection protection for databases, source code or other vulnerabilities), at the transport level (for example, in terms of encryption of passwords or lack of proper protection of ports for accessing a web application) or at the front-end application level (for example, the manner in which tokens are stored on the user's device for the login process).

Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.[3] This entails that any type of data, regardless of format (e.g. database, metadata, logs, files), location of storage or whether in transit or at rest falls under this definition.

"Perpetrator"[4] is defined as the person (individual or legal entity) that directly committed the actions that constitute a criminal offence.

[2] Article 1 of the Budapest Cybercrime Convention.

[3] Article 1 of the Budapest Cybercrime Convention.

[4] See article 46 of the Romanian criminal code.

"Accomplice"[5] is defined as the person (individual or legal entity) that, with intent, helps the perpetrator or makes it easier for the perpetrator to commit the criminal offence. An accomplice can either act before the perpetration occurs (e.g. leaving a back door access to an IT system for access in the future) or assistance is given to the perpetrator at the moment the perpetration takes place.

We continue with more legal concepts that are required in order to understand the conditions for criminal offence perpetration and in order to be able to set out workflows and awareness trainings that prevent such situations. This overview of legal concepts is followed by specific examples that reflect potential consequences to take into consideration in case of offensive security exercises.

In criminal law, it is important to determine if a criminal offence was perpetrated with intention or not. This is relevant, as some actions are considered criminal offences only if they are perpetrated with intention, whereas, other actions are considered criminal offences when perpetrated with intention or negligence. First, as an example, let us understand these two concept under Romanian law and, then, apply them to use cases for each type of criminal offence covered by this section. Their definition might differ slightly in each country, but, generally, the concepts include the below conditions.

"Intention"[6] is defined as the type of fault in perpetrating a criminal offence whereby:

- The perpetrator foresees the consequences of his/her/its actions, having the purpose of such consequences occurring (direct intent); or
- The perpetrator foresees the consequences of his/her/its actions and, even if not having as purpose such consequences, he/she/it accepts them (indirect intent).

"Negligence"[7] is defined as the type of fault in perpetrating a criminal offence whereby:

- The perpetrator foresees the consequences of his/her/its actions, but considers these will not occur (foreseeable negligence); or
- The perpetrator does not foresee the consequences of his/her/its actions, even if he/she/it should have (unforeseeable negligence).[8]

The above subjective nature of taking actions can be analysed by reference to the main individual performing the action or to individual assisting him/her. Under criminal law, individuals related to the perpetrating of a criminal offence can also be held liable (e.g. instigator, accomplice). Below we cover the cases of perpetrator and accomplice, which are to be encountered in the use cases described in this section.

Further, as an example, under Romanian law, legal entities[9] can become liable from a criminal law perspective, provided the conditions under the Romanian criminal law are fulfilled. Generally, a private entity can be held liable for criminal offences perpetrated by individuals related to its business activity or on its behalf or for its benefit. Thus, a legal entity can be a perpetrator or an accomplice, as defined below. There are legislations in certain countries that have a similar approach towards legal entities. However, there are also countries that do not provide for the liability of legal entities, but only of individuals.

After this brief background on the main concepts in criminal law, we are continuing the section with use cases that may be encountered in offensive security exercises and manner of preventing that they are potentially interpreted from a criminal law perspective. The use cases mentioned below are not meant to be exhaustive, but are the main ones that can be encountered in cyber offences in general. This

[5] See article 48 of the Romanian criminal code.

[6] See article 16 of the Romanian criminal code.

[7] See article 16 of the Romanian criminal code.

[8] Chandler, Jennifer A., Negligence Liability for Breaches of Data Security. Banking and Finance Law Review, Forthcoming. https://ssrn.com/abstract=998305 , last accessed on 28 February 2020.

[9] See article 135 of the Romanian criminal code.

is useful for both companies and offensive security service providers in order to identify examples to be included in awareness trainings and to be had in mind when interacting with IT systems.

The main criminal law implications derive from accessing IT systems/confidential data that should not be accessed under the service agreement, extracting data from the IT systems of the company without right and intercepting communication towards/from the IT systems of the company.

The most relevant criminal offence is the accessing of an IT system (including data therein) without a right. This criminal offence is meant at protecting the social relations related to the confidentiality of the data in the IT systems.[10] This data can belong to a company or to individuals (employees, customers, co-contractors of the company). Thus, this provision protects both the ownership of the entity owning the IT systems and the ownership of the data held on these IT systems. This ties in with the data protection legislation protecting the data in the IT systems.

The scope of this criminal offence refers to the components of the IT systems, from the hardware infrastructure to the databases and applications found within the IT systems, together with the data found in these components (including logs, metadata, data found in databases, unstructured data found on servers, cookies).

Further, the mere analysis of metadata, browsing history, types of cookies stored on the device, the types of apps installed on the device/their version, location, status of various sensors placed on the device and traffic data may also constitute unlawful access to an IT system, if there is no legal right or consent of the user to access such data.

The illegal accessing of an IT system includes various degrees of access: the authentication (entering the system as a user thereof), bypassing the authentication system (through various means, such as, brute force, social engineering), reading content in the IT system, copying/deleting data from the IT system or using the IT system to perpetrate other criminal offences. The legal provisions for this criminal offence include an aggravated version if the perpetrator surpasses certain security measures to enter the IT system (as, for instance, in the device monitoring context is found in some types of deep packet inspection). The legal doctrine is divided in terms of the need for such an aggravated version, as the impact on the rights of individuals is the same. The distinction between the usual type of perpetration and the aggravated criminal offence may be useful in correlation with obligations to ensure security measures are in place in an IT system. Thus, for the civil part of the litigation, the entity that did not ensure proper security measures for the IT system can be held liable for a part of the damages.

The transfer of data from the IT system also constitutes a criminal offence. This usually involves the prior access to the IT system. The transfer is unauthorised, in the sense that the perpetrator either does not have any legal or contractual right to transfer the data or the perpetrator exceeds its right to transfer data as part of its usual business activity or transfers the data to another location than in the course of its usual business activity. This entails the breach of the confidentiality and potentially integrity and availability of data (in case data is modified, deleted or there is a denial of service).

The criminal offence refers to the transfer of data outside of a given IT system (outside of, for example its databases, its storing spaces in case of data at rest or its infrastructure in case of data in transit).

There are certain specific situations in which there can be a violation of privacy. This criminal offence is rather new in Romanian legislation and case law is scares on the topic. Generally, it protects the social relation of one’s life from illegitimate intrusions from others, either through the taking of pictures or from the listening of private conversations by others. This is applicable in situations where the illegally accessed IT system involves interaction with users (clients) or with employees of the

[10] I.C. Spiridon, *Reflecţii cu privire la legislaţie română în domeniul criminalităţii informatice*, Dreptul, no. 6/2008.

company. In other jurisdictions this type of criminal offence may not be regulated. Thus, specific analysis of the relevant jurisdictions is necessary.

## 5. Use of third party tools in offensive security

There are certain situations in which, either the company or a service provider does not hold on premise licensed offensive security tools or self-built offensive security tools. In case of use of third party tools, these entities may opt to use third party tools that are hosted on the servers of such third parties.

This is generally the case of SMEs or certain cyber security start-ups as it is less expensive and swifter to set-up, whereas established international groups usually opt for on premise offensive tools or tools that they have built internally. Of course, in addition, there is a degree of privacy and security risks associated with using third party tools, as it involves another entity in the supply chain which gains access to confidential/personal data.

In case of using third party tool in offensive security, the main aspects to be considered by the company relate to liability, confidentiality and data protection, as detailed in this section.

Nevertheless, in case a service provider offers tools that can be used in offensive security, such service provider has to analyse the legal requirements that can be applicable to it and the active steps that it should take to fulfil such legal requirements. The main consequence that triggers this is the possibility of such tool being used for illegal activities.

Firstly, it is recommended to prohibit the use of the tools for illegal activities in the agreement that allows the use of the tools. However, it may considered that this is not enough to ensure lack of liability of the entity providing the offensive security tools. One solution might be to periodically verify the manner in which the tools are used and the existence of approval from the entities against which the tools are used. This monitoring might be useful in order for the entity providing the tools not be considered an accomplice to any criminal offences perpetrated by its clients, as it may be argued that the entity is acting with indirect intent.

Another factor to consider when providing such tools to entities for their use is that holding tools that can be used for criminal offenses on IT systems with the intent to perpetrate a criminal offence may be a criminal offence itself, depending on the applicable legislation. This is the case under Romanian law and similar criminal offences may be included by other jurisdictions. Of course, the intent has to be proven through any means available.

The provision of such penetration testing as a service (as detailed above) also entails the storing or confidential data that results from the offensive security tools used. This entails that the entities using the tools should guarantee that they have rights to store.

## 6. Specific commercial points to consider

Aside from the legal and commercial aspects mentioned above as relevant for analysis when concluded an agreement, there are certain commercial points concerning liability that have to be considered as well. The below details represent awareness of the various aspects to consider when drafting an agreement and should be reflected in the agreement on a case by case basis, depending on the specifics of the situation.

Clauses concerning liability of the parties in terms of manner of performance of the agreement (including specific requirements and limitations under the agreement) is essential in case of offensive security services.

Liability can stem from breach of contractual obligations (either intentionally or not), breach of legal provisions (in case legal requirements are incumbent on the service provider or in case of criminal offences) or tort liability (in case of actions that create a prejudice for the company).

Contractual liability entails that the service provider, intentionally or not, has not performed an action or has performed an action without respecting the contractual or legal requirements. This type of liability relates only to specific obligations undertaken under the contract.

Breach of legal provisions entail the existence of a specific legal obligation applicable directly or indirectly to the service provider. The breach of legal provisions can have an impact in terms of sanctions applied by public authorities and of damages to be paid by the service provider if it is determined that it is its fault for the damages incurred.

Tort liability entails that an action of the service provider is a direct link to damages incurred by the company or other third parties, such as the customers of the company. Generally, the employer (in this case the service provider) is liable for the actions of its employees during their work activities. Tort liability can occur in any circumstances and does not relate to the contractual relation between entities.

In view of transferring risk, the company can opt for an insurance policy to cover potential liability occurring from the actions of the service provider, with the insurance being provided by the service provider to the company.

Below, we have outlined a couple of use cases that can be debatable from a liability perspective and potential approaches from a contractual drafting perspective. This is useful in view of illustrating the various aspects to consider when concluding an agreement.

- The service provider performed actions in addition to the scope of work. Generally, this should not result in liability of the service provider, provided other contractual obligations or tort damages are generated by such actions.
- The service provider did not perform the actions under the scope of work (either did not provide all actions or did not provide them properly). This can generate contractual liability.
- The service provider delivered an incomplete advice in terms of the scope of work needed in order to cover the legal requirements for offensive security testing. This can be rather difficult to establish, as it always requires the scope of work concerning consultancy to have been included in the service agreement. Further, there is the question of legal interpretation for the duty of care and negligence of the service provider in providing such guidance. The legal interpretation depends on a case by case basis and may be influenced on whether a lawyer was involved in the analysis or not.
- The service provider unintentionally created damages to the company (or to third parties) or generated a security incident through their performance of the testing. Examples in this respect include: accidentally running malware found on the company's IT system, accidentally, accidentally created a DoS for the IT systems of the company or its clients. In certain cases, the service provider can even be held liable for unintentional damages. However, this depends on the contractual provisions (whether such liability was undertaken by the service provider under the contract) and on legal obligations of the service provider under the applicable law.
- The service provider intentionally created damages to the company (or to third parties) or generated a security incident/eased the access of attackers through their performance of the testing (including extracting confidential data). This situation is generally covered by the service agreement, as it is closely correlated with the scope of work.
- The report did not reflect properly the impact or the probability of a risk, as this is usually perceived in the industry based on past events. The adequate risk assessment and risk rating depending on industry and best practices in a specific field is generally essential for companies

to prioritise investments in security controls. This is closely tied to the proper performance of actions as required by the service agreement and legislation requiring a specific level of security.

- Damages generated by the automatic tool used during the testing exercise, including any machine learning or similar tools. One should analyse the amount of knowledge of the entity that used the automatic tool or lack of knowledge in order to determine liability.
- Leaving eavesdropping tools or similar tools in the IT systems of the company for future monitoring or extraction of information from these IT systems. This is generally performed with intent and falls under contractual liability general, but also may involve tort liability and legal liability (especially in case of criminal law angles).

Under Romanian law, certain types of damages cannot be excluded, such as the following:

- Material damages caused through intent or gross negligence.
- Damages concerning physical integrity, emotional integrity or health of an individual.

Depending on the applicable jurisdiction, similar or other exclusions may be applicable.

As the actual offensive security testing is performed by individuals, either employees of the service provider or external consultants thereof can be involved in the process. Thus, it is worth having a guarantee from the service provider that the employees/external providers are aware of the obligations undertaken under the contract or, alternatively, the employees/external providers can acknowledge and agree to such obligations directly.

An interesting situation from a legal perspective is the limitation of liability for damages generated by the company on the IT system of the service provider (e.g. malware that gets transferred to the IT systems of the service provider). This can be limited to situations in which this damage was created with intent.

In terms of limiting the liability of the service provider, there are certain points that can be included in the offensive security contract:

- Amount of damages covered – the amount can be negotiated between the parties.
- Limitation of actions for which the service provider is responsible – some of the above actions can be limited, including intent of actions.
- Limitation of damages covered by the liability clause – generally, direct damages resulting directly from the actions of the service provider are covered by service providers. Also, some indirect damages – loss of profit, costs with lawyers, litigation costs are sometimes included.

Liability clauses in an agreement are mainly a commercial point that has to be discussed and agreed between the parties. Nevertheless, it is essential to have a full picture of the potential implications of actions taken by each party, in order to tailor accurately the liability clauses.