



**White hat hackers:
 their legal position, the risks they take
 and the role of the FDPIC**

I. Purpose1

II. Background and definitions.....1

 1. White hat hacker (WHH).....1

 2. Coordinated vulnerability disclosure (CVD).....2

 3. The CVD policy implemented by the NCSC2

III. Legal situation of white hat hackers under the FADP.....2

IV. Legal risks for white hat hackers3

 1. Risks under civil law (in particular Art. 32 FADP)3

 2. Risks under criminal law (in particular Art. 143, Art. 143^{bis} and Art. 179^{novies} SCC)3

 3. Risks under administrative law (FDPIC, Art. 49 ff. FADP).....4

V. Role of the FDPIC4

I. Purpose

- 1 This information sheet is aimed primarily at white hat hackers. It aims to raise awareness of the nature of their activities in relation to the legal framework in which they operate, particularly with regard to data protection. This information sheet is not intended to make a judgement on these activities, but simply notes that white hat hackers do exist and that they should therefore receive guidance regarding their activities.

II. Background and definitions

1. White hat hacker (WHH)
- 2 The Federal Data Protection and Information Commissioner (FDPIC) and the media are increasingly receiving information that vulnerabilities have been discovered in IT systems. These announcements are often made by people who describe themselves as ethical hackers (White hat hackers, hereinafter «WHH»). WHHs ideally work to detect vulnerabilities in a helpful way: they will not seek to exploit them for gain, or to use them to benefit a particular cause (cyber activist or «hactivist»). On the contrary, they enable the system operator to fix these vulnerabilities and improve its IT security. WHHs are sometimes hired by the system operator to test the system: these cases of cooperation are usually harmless by nature and therefore do not fall within the scope of this information sheet.
- 3 The explanations that follow are aimed at WHHs that act outside any framework and without the knowledge of the system operator, who will only be informed if a flaw is actually found. This type of

activity is often at risk of breaching the law. Without claiming to be exhaustive, this information sheet aims to provide some thought-provoking impulses, so that WHHs are in a better position to assess the implications of their actions. The perspective adopted here is that of a WHH in its ideal form, someone wanting to do the right thing. The activities of hackers who aim to gain a direct advantage (e.g. exploiting data for their own purposes) or those of activists, who use these flaws for protest purposes (e.g. blocking a company's website), are fundamentally incompatible with the prescriptions that follow (chapter 3.4 of the [NCSC report of 16 February 2021: General forms of threats, perpetrators and tools](#) provides a broadly defined concept of hacktivists, independent of questions of malice/benevolence).

2. Coordinated vulnerability disclosure (CVD)

- 4 Coordinated vulnerability disclosure (CVD) refers to the process of coordinating and sharing information on vulnerabilities among relevant stakeholders (those who discovered the vulnerability, the companies affected, governmental computer emergency response teams [CERT]) with the aim of reducing the negative effects of vulnerabilities and informing the public. A CVD policy includes setting up reporting platforms where WHHs can report any security flaws they discover without fear of legal action, and also generally requires system operators to remedy any flaws reported within a set period¹.
- 5 CVD essentially runs counter to the recognised premise codified in Article 2 of the [Budapest Convention on Cybercrime of 23 November 2001 \(SR 0.311.43\)](#), which states that signatory states shall take legislative measures to establish intentional unauthorised access to a system as a criminal offence. This may explain why the Netherlands and France are the only European Union member states with a fully developed CVD policy².

3. The CVD policy implemented by the NCSC

- 6 In Switzerland, the National Centre for Cyber Security (NCSC) has set up a CVD reporting platform³ and a best practice information sheet designed to guide WHHs. Generally these rules are also relevant with respect to data protection law; this information sheet is complementary and focuses on certain specific aspects of data protection.

III. **Legal situation of white hat hackers under the FADP**

- 7 Accessing a computer system by exploiting a vulnerability often provides access to the data it contains. In the case of personal data, the Federal Act on Data Protection (FADP)⁴ applies. Any operation that the WHH carries out with this data – consultation, downloading, disclosure, recording etc. – constitutes processing within the meaning of the FADP (Art. 5 let. d FADP). The FADP lays down a number of essential principles that all data processors, including WHHs, must respect.
- 8 If they fail to do so, they must be aware that their data processing activities are inherently unlawful, even if they are acting as a completely ethical WHH. The following principles are some of the most relevant to WHH activities:
 - The principle of lawfulness (Art. 6 para. 1 FADP) involves compliance with legal requirements including those outside the FADP: processing is unlawful if it infringes a legal rule. This principle clearly applies to criminal law (e.g. Art. 138 ff. or Art. 179 ff. of the Criminal Code [SCC]), but more

¹ [Governance of 0-day vulnerabilities in German cybersecurity policy – German Institute for International and Security Affairs \(swp-berlin.org\)](#), p. 32, accessed on 25 May 2023.

² [Governance of 0-day vulnerabilities in German cybersecurity policy – German Institute for International and Security Affairs \(swp-berlin.org\)](#), pp. 33-34, accessed on 25 May 2023

³ [Coordinated vulnerability disclosure \(CVD\) \(admin.ch\)](#), accessed on 25 May 2023.

⁴ In the present paper, when the FADP is cited, reference is made to the new law, which will come into force on 1st September 2023.

broadly to the legal system as a whole (e.g. the prohibition of deception or threats under Art. 28 ff. of the Code of Obligations [CO]).

- The principle of good faith (Art. 6 para. 2 FADP) refers to the general conduct of the person processing the data. For WHHs, this means in particular not having a hidden agenda and not seeking to harm the system operator or the people concerned. They must not do anything that would hinder the system operator's efforts to fix the vulnerabilities that have been discovered and (re)establish compliance with data protection requirements. This includes making threats, setting unrealistic time limits or blocking systems.
- In accordance with the principle of purpose (Art. 6 para. 3 FADP), data must not be used for purposes that are incompatible with the objectives given at the time of collection. Data processing by a third party such as a hacker, even if well-intentioned, is inherently incompatible with the initial objective of collecting the data. The processing is therefore unlawful in principle. It is essential that WHHs refrain from processing any personal data that they are able to access.
- The principle of proportionality (Art. 6 para. 2 FADP) requires that no more be done than what is necessary to achieve the intended objective – in this case, to diagnose and document the vulnerability (proof of concept). If a WHH considers it necessary to access the data themselves for their investigations, despite the probable unlawfulness of this action, they should minimise their data processing activities both in terms of data quantities and the type of processing. This also means that they must not keep the data any longer than necessary. The NCSC's recommendation to carry out processing only on one's own profile is particularly relevant here (see point 6 above).
- These principles also prohibit communicating the data that has been exposed, or disclosing the existence of the vulnerability (except to the supervisory authorities), which could harm the people concerned (those whose data is affected). Thus, disclosure in the media before the flaw has been fixed is a priori incompatible with these principles, particularly when the system operator is trying to fix the vulnerabilities as quickly as possible. Similarly, these principles require WHHs to inform the system operator of their discoveries as soon as possible, and to give the operator sufficient time to fix any vulnerabilities.

IV. Legal risks for white hat hackers

1. Risks under civil law (in particular Art. 32 FADP)

- 9 WHHs' activities may lead them to infringe the above principles, exposing them to civil claims from the system operator or the people concerned. If they act in good faith and limit their processing to a minimum – in other words, if they are acting as an ideal WHH and striving to comply with the principles of the FDPA – it can be assumed that there will be no real interest in bringing legal action. By the time the system operator or data subjects have been informed of the vulnerability, the WHH will have already deleted any data collected or will be in the process of doing so, and since the WHH will not have disclosed any information, there will be no economic or reputational damage, etc.
- 10 The risk of civil action cannot be ruled out – it is the decision of the operator and the people concerned – but ideal conduct by the WHH will minimise these risks.

2. Risks under criminal law (in particular Art. 143, Art. 143^{bis} and Art. 179^{novies} SCC)

- 11 In addition to the civil risks, WHHs are exposed to the risk of criminal prosecution, in particular on the basis of Articles 143, 143^{bis} and 179^{novies} SCC. Some of these behaviours are by definition incompatible with a WHH (e.g. Art. 143 para. 1 SCC, where the hacker's aim is to enrich themselves). Others can be committed even if the hacker behaves in an ideal manner (in particular Art. 143^{bis} para. 1 and Art. 179^{novies} SCC). As the latter offences are as a rule only prosecuted on complaint, the considerations related to mitigating the risks of civil action also apply here.

12 Furthermore, when there is a well-founded suspicion of offences being prosecuted *ex officio* (i.e. even in the absence of a complaint), FDPIC staff have a duty to report (Art. 22a of the Federal Personnel Act [FPA]).

3. Risks under administrative law (FDPIC, Art. 49 ff. FADP)

13 When processing data, WHHs may become data controllers themselves within the meaning of the FADP. If their conduct appears not to comply with the FADP, especially if it appears that the hacker has not endeavoured to comply with the principles mentioned above, the FDPIC can open an investigation and order administrative measures against the WHH (Art. 49 ff. FADP).

V. Role of the FDPIC

14 An announcement to the FDPIC by the WHH is not compulsory and indeed is not specifically provided by the FADP (unlike the data controller, who is obliged to announce when a breach poses a high risk to data subjects, in particular when there is a risk that the breach may have been exploited - see Art. 24 FADP). If a WHH nevertheless plans to inform the FDPIC, there are several factors to consider:

- As mentioned in point 12 above, when there is a well-founded suspicion of offences being prosecuted *ex officio* (i.e. even in the absence of a complaint e.g. Art. 143 para. 1 SCC), FDPIC staff have a duty to report (Art. 22a FPA).
- If there is sufficient evidence of a breach of data protection provisions, the FDPIC may open an investigation (Art. 49 ff. FADP) against the controller according to Art. 5 lit. j FADP (e.g. the system operator). If data protection provisions are breached, he may order administrative measures to remedy the data protection risks (see Art. 51 para. 3 FADP). Nevertheless, it may not always seem appropriate to provide this information to the FDPIC. If the vulnerability is not the result of gross negligence, there is no indication that it has been exploited, and the system operator remedies it adequately, there may be no need to open an investigation.
- Finally, the FDPIC can open an investigation (Art. 49 ff. FADP) against the hackers themselves. It should also be pointed out that the FDPIC does not offer a guarantee of anonymity to the WHHs, although disclosure of the name by the FDPIC will always be for a specific purpose and within the legal framework.