

*Guidelines for*  
**IT, Data, and Service Providers**  
**State Searches as an Important**  
**Component of IT Security Policy**

**We promote competencies.**  
**We create transparency.**







## Publication Details

EuroCloud Deutschland\_eco e. V.  
Lichtstrasse 43h  
50825 Cologne  
Phone: +49 (0)221 70 00 48 – 0  
Fax: +49 (0)221 70 00 48 – 111  
Email: [info@eurocloud.de](mailto:info@eurocloud.de)  
Web: [www.eurocloud.de](http://www.eurocloud.de)

Register of Associations:  
District Court (Amtsgericht) Cologne – VR 16215

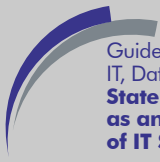
Registered Office:  
Cologne

Jointly published with:  
Derra, Meyer & Partner Rechtsanwälte PartGmbB



## Contents

Preface	5
1. To Begin: General Rules of the Game	6
1.1 Basis of the state search	6
1.2 Accused party - Silence is golden	6
1.3 Third party/ witness – Immediate questioning of witnesses is inadmissible	7
1.4 From witness to accused party – possible at any time	8
2 Start of the Search: First Steps	9
2.1 Demonstrate decisiveness	9
2.2 Check content and, if applicable, register any discrepancies	9
2.3 Right to be present	9
2.4 Contact lawyer	10
3 During the Search	10
3.1 Delimit information as much as possible	10
3.2 Cooperate – but remain silent	10
3.3 Premise owner’s rights: No questioning of witnesses!	11
3.4 Accompanying the search	11
3.5 Making copies	11
4 Conclusion of the Search	12
4.1 Do not voluntarily hand over documents	12
4.2 Objects/data found – Inventory of seizures	12
4.3 Internal closing meeting	12
5 Checklist: Procedure for Search Measures	13
6 Requests for Information	13
7 Special Case: Secrecy of Telecommunications	15
8 Tension Between Legal Obligation and Contractual Obligations Towards Customers	16
9 The Right Preparation	17
9.1 Classifying services – Separating data	17
9.2 Test run absolutely necessary	17
9.3 Important parameters	18
10 Dealing with “Requests to Preserve Evidence” by Law Enforcement Authorities	19
11 Knowledge of Criminally-Relevant Information	19
11.1 Check duty of disclosure	19
11.2 Establishing codes of conduct	20
11.3 eco Complaints Office – Options for reporting to non-police body	20
Authors	22





## Preface

Dear Readers,

When the prosecutor appears at your door to search your premises, it's invariably unannounced. The same goes for the police, tax or customs officer, and other investigative authorities, each with their respective judicial search warrant. What are they allowed access to and how do you manage the balancing act between cooperation and your obligations to your customers?

These guidelines clarify your rights and duties, and prepare you for an emergency, so that if one comes, you can react calmly and sensibly. Here, you need to be clear: The investigations signify a legal disruption of the technical and organizational measures that are designed to protect your IT from attacks and outages. Depending on the process, the state search can have the same impact as an IT security incident. This is why you should view the preparation for a state search as a component of your IT security policy.

These guidelines focus primarily on the situation in which your company – or bodies or executives within your company (Board, CEO) – does not stand as an accused party, but rather as someone duty-bound to provide information. Generally, the bodies or staff of the company then take a role as witnesses in an investigation against a third party.

The guidelines concentrate above all on IT, data, and service providers. Whether you belong to the circle of potential affected parties that come in contact with the investigative authorities depends on which services you offer and who your customers or contractor are. Hosting providers and Internet access providers are certainly more frequently contacted by investigative authorities than the providers of call-center services, for example. But if it gets serious, the situation is the same for everyone ...

We wish you many valuable insights in reading these guidelines and would like to sincerely thank the authors for their engaged involvement.

Cologne, 1 March 2018



Andreas Weiss  
Director, EuroCloud Deutschland\_eco e. V.

## 1. To Begin: General Rules of the Game

### 1.1 Basis of the state search

For criminal investigations, the public prosecutor is exclusively responsible as “chief of the investigation”. For its investigative work, the public prosecutor’s office employs the investigating officers of the police force.

According to the so-called “principle of legality”, the public prosecutor’s office is legally obliged to initiate an investigation procedure or at least to conduct preliminary investigations as soon as it becomes aware of possible criminal offenses. This is done as a rule through bringing criminal charges. As soon as the police identify a person during their investigations who they consider to be the suspected or accused party, they must make him/her aware of this and inform him/her of his/her rights.

If the relevant legal requirements are met, searches, associated seizures, and the confiscation of objects and data which could be produced as evidence can be ordered by the investigating magistrate both for the party accused of a criminal offense (§ 102 StPO – German Criminal Code) and for a non-suspected third party (§ 103 StPO – German Criminal Code).

The decisive factor for the legal situation in carrying out the search is whether you are affected as the accused party or as a witness/non-suspected third party, because this determines your associated rights and obligations. You can ascertain this information from the judicial search warrant, and observance is mandatory for the investigative authorities. Searches of uninvolved third parties are subject to much stricter legal requirements than searches of suspected parties, in particular in the context of the proportionality of such a compulsory measure.

### 1.2 Accused party - Silence is golden

For the accused party, one of the most elementary rights is the fundamental protected right not to have to incriminate oneself and thus the right to remain silent. In addition, the accused party has the right to consult an attorney as a defense lawyer for any part of the proceedings. These rights should be exercised at all costs! The basic principles apply: Silence is golden, and consult a defense lawyer before you talk to the investigating officers!

Nothing is so important that the officials must be immediately deferred to without legal assistance. Of course, you are subject to the legal obligation to allow such a search and you are not entitled to oppose police measures or orders. Otherwise, you could become liable to prosecution for resisting law enforcement officers. However, no one is compelled to actively participate.

It is therefore advisable within the framework of the search not to voluntarily provide any information, nor to otherwise actively participate in an investigation.

However, for providers in particular, this is a fine balancing act, because a certain assistance to the investigators can serve to ward off detrimental effects for customers who are not affected by the search. The provider is contractually obliged to protect its customers. If the provider is not prepared for the measure and this leads to damage to customers against whom the investigative measure is not directed, a liability risk exists for the provider.

The provider must therefore consider investigative measures in two respects – on the one hand, as part of the planning of its service provision in order to be prepared; and on the other hand, in concrete situations, when it comes to a search operation. The basis for both is to familiarize oneself with the legal framework, to define and test the measures.

### 1.3 Third party/ witness – Immediate questioning of witnesses is inadmissible

As a third party/ witness, you are obliged by law to provide complete and truthful information to the law enforcement authorities. False statements can lead to criminal proceedings for attempted obstruction of justice or unsworn false testimony or perjury, in some cases with high penalties.

But here, too, you are never immediately obligated to make a statement and may always first consult a lawyer. According to the reform of the German Criminal Code (StPO) which came into force on 24.08.2017, a witness is obliged to present himself or herself to the police when summoned and to testify on the matter if the summons is based on an order issued by the public prosecutor's office (§ 163 Para. 3 Clause 1 of the StPO - German Criminal Code). Immediate questioning of witnesses conducted as part of a search, however, remains inadmissible, as the prerequisites for a proper summons are usually lacking. According to this provision, the police force equates to an investigating officer of the public prosecutor's office, i.e. in addition to police officers in the narrow sense, it also covers investigating officers of the customs office and the tax office (§ 399 AO – Regulation of Taxation). In case of doubt, consult your legal adviser.

Furthermore, not every witness is obliged to testify. In investigative proceedings against close relatives (parents, grandparents, children, spouse, fiancée, etc.), there exists a right to refuse to testify for personal reasons. This means that the witness may refuse to give any testimony regarding the accused close relative. Furthermore, no one has to incriminate himself or herself of criminal behavior. Each witness can therefore refuse to answer questions that would expose himself or herself or a close relative to the risk of criminal prosecution.

Likewise, professional privilege carriers (e.g. defense lawyers, doctors, tax consultants, attorneys, clergy) are legally bound to secrecy and have the right to refuse to testify. They have certain privileges to protect against state access, which is intended to protect the relationship of trust between the data subject and the professional privilege carrier. Under no circumstances should you exempt them from their obligation to secrecy – at least not without first obtaining legal advice on the significance and impact of this.

The level of protection afforded to professional privilege carriers varies. However, it does not automatically and always extend to providers. This means that, in the case of a provider, the same data is not subject to special privileges and could be confiscated. This should be clarified explicitly with relevant customers in order to avoid unpleasant surprises.

The Telemedia Act (TMG) provides in §§ 7 to 10 for so-called liability privileges for host, cache, and Internet access providers. However, these regulations do not apply to criminal investigative measures. In other words, they do not merit as a valid “defense” against an investigative measure. They are therefore not relevant to the subject of these guidelines. However, the regulations are relevant when it comes to possible criminal liability of host, cache, and Internet access providers for content found on their sites.

If there is any doubt concerning a possible right to refuse to testify as a witness, an experienced defense lawyer should always be consulted. This is the only way to avoid the danger of an imprudent possible self-incrimination of oneself and relatives.

#### 1.4 From witness to accused party – possible at any time

Caution: During the ongoing investigation, a switch from being a witness to that of an accused party could occur at any time; for example, if you have been searched as a non-suspected party, or a witness hearing has begun. As soon as there are indications of a charge of a criminal offense, the party concerned must be informed of this and informed of his/her rights.

Therefore, even though you are generally affected as a third party, you must carry out the preventive preparations and the measures to protect your customers for both configurations.



## 2 Start of the Search: First Steps

Regardless of whether it's the police or the public prosecutor's office who's ringing at your door with a search warrant: At this point, a search can no longer be averted and active resistance could possibly be indictable. Nevertheless, not only should you protect your own rights – as a service provider you must also keep the rights of your customers in your sights. A search for evidence is always unpleasant – for everyone involved. This is also a tense situation for the investigators at the beginning, as they do not know what to expect. Ease the tension of the situation by assuming a calm and objective approach!

### 2.1 Demonstrate decisiveness

Invite the investigators into an empty room and request contact with the leading investigating officer. Since a search may only be carried out on the basis of a court order, the investigators must first be requested – courteously – to present their ID cards and the search warrant. From this the object of the search can be ascertained, i.e. what is being looked for and where will be searched. Here you will also find the answer to the critical question as to whether you are affected as an accused party or as a witness, because that will dictate your rights and obligations. The investigative authorities cannot leave you in the dark about this. If the search warrant does not give you clarity, ask the leading investigating officer, and be prepared for the eventuality of this status changing at any time.

### 2.2 Check content and, if applicable, register any discrepancies

Make sure that the warrant is addressed to your company and that the named premises to which the search pertains are stated with the correct address. If the name or address is not correct, inform the officials on the scene and insist on objecting to the search on the grounds of this/these discrepancy(ies). Document this objection in writing and ask the search officials to record the objection. The rooms named in the warrant must nevertheless be shown to them willingly.

### 2.3 Right to be present

The party subject to a search has the right to be present during the search and should without question avail of this right. A secret search is not permitted. The management or an official authorized for such situations and responsible to management should be immediately informed. The customer against whom the measure is directed, however, has no right to be present. They also do not have to be informed by the investigative authorities in advance or in the course of the action. By contacting the customer, the provider risks being accused of obstructing the course of justice if the customer is being investigated as the accused party (this may be indictable under criminal law). In

order to ward off any discussion with the customer about possible (ancillary) contractual obligations to provide information, it may be advisable to clarify in the contract with the customer that such an obligation to provide information does not exist under any circumstances.

#### 2.4 Contact lawyer

Telephone contact with a lawyer may not be refused. If the investigators profess the opinion that a telephone call would endanger the result of the investigation, insist that an investigating officer call the designated lawyer before the search begins. If a lawyer can be reached, the leader of the search should be asked to wait until the lawyer arrives before carrying out the search. But be aware that there is no right to this: as such, if for no other reason, a polite tone is recommended.

### 3 During the Search

#### 3.1 Delimit information as much as possible

If you are the party responsible for providing the information, the warrant is usually limited to certain information, certain documents, or certain data relating to the accused party. In order to avoid a general search and the extensive adverse effect on your company that this would entail, it is advisable to delimit the information requested. This is also done to protect your other customers because, in the absence of a cooperating delimitation, everything will be searched. Civil law collateral damage must be avoided here. Unfortunately, there is no general advice for the procedure to be chosen. The circumstances of each individual case must always be taken into account.

If the assessment of the particular case allows for a cooperative approach, you may, in consultation with the officials, make specific copies or images of the data carriers or documents in question, provided that this does not also result in the release of data from other customers (see also Sections 8 and 9.1). If you cooperate, the principle of proportionality especially applies to the investigators, according to which no unnecessary damage may be inflicted on your company. The attempt to secretly destroy documents or delete data during or immediately before the search may, if discovered, immediately lead to imprisonment for the accused party (danger of collusion) and represent an (attempted) obstruction of justice for a third party.

#### 3.2 Cooperate – but remain silent

In general, cooperation should be established with the investigators – unless the content of the search warrant seems to have “sprung out of nowhere” (e.g.

in case of a mix-up). However, the extent of the cooperation should be limited to polite and friendly behavior. Pending consultation with a defense lawyer, you should **under no circumstances** divulge information on the matter at hand – even in the case of persistent enquiries.

Aside from the accused party, who does not have to provide any information at any time in criminal proceedings, witnesses are also always entitled to talk with a lawyer before making a statement. In addition, witnesses are only obliged to testify before a public prosecutor or a judge. Whereas, since the reform of the German Criminal Code, there is also an obligation to testify to the police on the basis of a court order, within such a search warrant the required court order according to specification is typically lacking.

Just as the accused party has a complete right to remain silent, relatives of the accused party have a right to refuse to testify. In addition, all parties have the right to refuse to provide information in order to protect themselves from self-incrimination – for example, if the possibility arises that they could be considered to have aided and abetted an offense that is the subject of the investigation. You can find more detailed information on this subject in Sections 1.2 and 1.3.

### 3.3 Premise owner's rights: No questioning of witnesses!

Investigators like to exploit the commotion of a search situation to try to examine witnesses directly and unprepared at the scene. Irrespective of the rights to remain silent already described, the owner of the premises can prohibit such a questioning of witnesses on their premises – the search warrant does not grant an entitlement to questioning witnesses.

### 3.4 Accompanying the search

The investigators must be accompanied at every step of their search actions by employees and are not entitled to operate the IT themselves. Every action should be recorded in its entirety. In order to avoid a “haphazard” search of all storage locations and the removal of more objects than necessary, it is advisable to show the investigators the objects they are looking for, and if necessary also to specify passwords, etc. All items of evidence found should be brought to a central location.

### 3.5 Making copies

When a business premises is being searched, care must be taken to ensure that business operations can be maintained even if certain objects or documents are removed. This must be pointed out to the leading investigating officer and duplicates must be requested.

## 4 Conclusion of the Search

### 4.1 Do not voluntarily hand over documents

Irrespective of the cooperative behavior during the search, you should always object to the seizure of documents. This compels the investigating authorities to formally confiscate the documents. Only then will the party concerned have legal recourse to a subsequent review of the legality of the seizure by the court. This is not possible if the requested documents are handed over voluntarily. This step is therefore decisive when it comes to your rights later and it is important when you have to explain to your customers why their data is held by the law enforcement authorities.

### 4.2 Objects/data found – Inventory of seizures

In a closing discussion – if possible in the presence of a lawyer – you should clarify with the officials what needs to be removed, and where making duplicates (copies, data backups, etc.) is sufficient. Ask the leading investigating officer for the detailed documentation of the confiscated or seized objects and documents (“Inventory of Seizures”). This is a right that you should not waive under any circumstances. Make sure that the items seized in the inventory are specifically, meticulously, and identifiably marked. Here, an exact description must be sought so that, at all times, the documents that are in the possession of the investigative authority can be traced.

### 4.3 Internal closing meeting

Once the investigating officers have left the company, a meeting should be held with all employees who accompanied the search. Here, the minutes of the meetings should be evaluated and the proceedings of the closing meeting should in turn be recorded.

## 5 Checklist: Procedure for Search Measures

If a search is carried out, rules must be observed. These rules should be defined in a corresponding plan or protocol for the company and should be imparted to the employees. There are different variants, but some rules should always be observed:

- Have the court order shown to you and check: Is the information correct? Are you the accused party (§ 102 StPO - German Criminal Code) or a third party (§ 103 StPO - German Criminal Code)?
- Inform management and lawyer.
- Cooperate - but remain silent!
- No investigating officer should work without an accompanying person from your company, who should keep a complete record of the proceedings.
- The investigating officers do not operate the IT themselves. This is done by an employee of your company in the presence of the investigating officers.
- The following applies to the company: Maintain your premises owner's rights! As a rule, no discussions between investigating officers and employees are permitted in the course of the search. Interviews and the questioning of witnesses should take place separately and with a clear time interval after the search and, if so, only in the presence of a lawyer.
- The following applies to employees: Questioning of witnesses and interviews are not permitted. Accused parties refer to their right to silence. Witnesses refer to their right to consult a lawyer and not to have to make any statements to the police during the ongoing search – without a proper summons.
- Make copies.
- Do not voluntarily surrender anything; instead, object to seizure and confiscation.
- Have the objection noted in the search protocol.
- Have the list of seized and/or confiscated items and data checked and submitted.
- After the search: Internal meeting of the employees involved, record minutes.

## 6 Requests for Information

As already noted above, the search of third parties (§ 103 of the StPO - German Criminal Code) is subject to very strict legal requirements. Therefore, within the framework of the proportionality of such compulsory measures, it is in general necessary, **prior to such a search of uninvolved third parties**, to request the voluntary handover of the searched objects/data on the basis of a written request for information by the police, public prosecutor's office, or court. Only in exceptional cases, where the purpose of the investigation requires a so-called undercover measure, is such a written request for information superfluous in averting a search.

However, the written request for information only applies before searches of third parties and uninvolved witnesses. In the case of accused parties, a search is always carried out without prior notice as a covert compulsory measure to find evidence and/or arrest the person.

If the authorities approach you with a written request for information, this is covered by the general right of investigation and constitutes an informal form of questioning witnesses. Aside from the information on data stored under §§ 95 and 111 of the Telecommunications Act (TKG) (cf. § 100j StPO – German Criminal Code), such a request for information cannot be enforced. But this does not mean that you must or should escalate the matter. Here, too, it is necessary to make a balanced assessment for the individual case at hand. If a request for information is not complied with, the next escalation stage is a search warrant or the questioning of witnesses.

If you decide to respond to the request for information, you must check what information is involved. If you are dealing with data that is subject to telecommunications secrecy, you cannot simply provide the requested information. You can find out more about this in Chapter 7.

Furthermore, you should be cautious when data from customers, especially sensitive data, is involved. This could give rise to a threat of claims for damages. In this case, it is better to refuse information and insist on a search warrant or a witness hearing. It must then be communicated to the requesting authority that the request for information does not constitute a sufficient legal basis and that further steps are therefore necessary.

Occasionally, in this context, the public prosecutor's offices also issue in advance search and seizure orders that they have previously obtained. However, these will only be enforced if the information is not provided.

But take care: If you now provide the requested information in order to avoid the measure, you must make it clear in writing that you are not doing this voluntarily, but only to avert the compulsory measure. The same applies to the summons for a witness hearing. Here it must be emphasized once again that according to the reform of the German Criminal Code, which came into force on 24 August 2017, a witness is also obliged to appear at the police station on summons and to testify on the merits of the case if the summons is based on an order issued by the public prosecutor's office (§ 163 Paragraph 3 Sentence 1 of the StPO – German Criminal Code). However, it should always be the practice to be accompanied by a legal counsel during any hearing.

## 7 Special Case: Secrecy of Telecommunications

The content and the detailed circumstances of telecommunications are protected by Art. 10 of the German Constitution and § 206 of the StPO (German Criminal Code). However, the obligation to protect only affects the telecommunications service provider, not the telecommunications participants.

In the case of data protected by telecommunications secrecy, it must be examined whether the investigative measure of the law enforcement authorities is the correct one. Case law on this subject has now become very differentiated, which is why no schematic answers can be given. However, the following key statements apply:

- Sections 111 et seq. of the Telecommunications Act (TKG) contain special provisions for the storage and retention of inventory and traffic data for information purposes. These regulations and the criticism levelled at them are not the subject of this guide. The following deals merely with access to this data.
- According to § 113 of the Telecommunications Act (TKG), information on inventory data may be requested if the company does not participate in the so-called automated information procedure. This information may also be requested by the police on the basis of § 113 of the Telecommunications Act (TKG).
- Information on traffic data is specifically regulated in the German Criminal Code (StPO). It ordinarily requires a court order and can be ordered by the public prosecutor's office in an emergency.
- Access to telecommunications content is also regulated in the German Criminal Code (StPO). This also ordinarily requires a court order and can be ordered by the public prosecutor's office in an emergency.
- However, the problem also exists that, over the past 10 years, the judiciary has increasingly expanded the demarcation of the boundaries from a narrow interpretation of the regulations. The judiciary justifies this by stating that the increasing shift of communication to electronic communication must not lead to the possibility of investigation being restricted. This means, for example, that in particular sets of circumstances, access to telecommunications content by way of confiscation has been permitted instead of by means of a telecommunications surveillance order, or disclosure of IP addresses has been based on the general investigative powers of the public prosecutor's office.
- For cloud providers, a particularity is that the use of their services takes place via telecommunications connections, but that their service itself (with the exception of Communication as a Service) is typically not a telecommunications one. When it comes to access and information, therefore, the decisive factor is where the investigative authorities start: on the telecommunications connection or on the storage systems. This determines which legal framework applies.

**This means: You must have clarified in advance whether and how the data is to be treated legally; which information you could be asked for; and under which conditions what data must and therefore may be disclosed.**

The dilemma with these data consists in the fact that an unjustifiably refused disclosure gives rise to significant vexation and the threat of a penalty due to (attempted) obstruction of justice. If, on the other hand, you disclose the data unjustifiably, a penalty according to § 206 of the German Penal Code (StGB) could be pending for a violation of the protection of the secrecy of telecommunications. But beware: Despite your obligation to protect, you may not object to a search!

## 8 Tension Between Legal Obligation and Contractual Obligations Towards Customers

The obligations under the German Criminal Code (StPO) conflict with the interests of the customer. A distinction must be made between the customer against whom the investigative measure is directed and all other customers.

For the provider, it is crucial to prevent an impact on other customers or to minimize this insofar as possible and to thereby counter the liability risk, by means of appropriate preparation for the possible search, seizure, or request for information, as well as through appropriate conduct in the specific case at hand. This requires a fine balancing act. If the criminal procedural duties alone are observed and the officials do not acquire any further information, liability towards the customer against whom the measure is directed is typically ruled out.

However, if with such a measure the investigating officers, with this increased access, also gain access to the data of other customers, this can present a problem. This extended knowledge can be used by the authorities against the customers.

A further problem is if the search leads to impairment or even outage of the services used by customers because, for example, hardware is seized. This can happen in individual cases, although the investigative authorities usually have to avoid this due to the principle of proportionality. What happens and how it happens ultimately depends on the circumstances of the specific case. An outage or loss of data can usually be prevented by appropriate redundancies or backups. If this is not the case, this should be clarified contractually.



## 9 The Right Preparation

Being prepared is good for both sides. If you are well prepared for investigative measures, less stress will ensue. You will avoid mistakes and the matter will proceed more quickly and “with less fuss”, which in turn saves time and money.

### 9.1 Classifying services – Separating data

The correct preparation necessitates the assessment and classification of your own services. “One size fits all” does not work here. On this basis, from a legal point of view, the risk constellations must be determined and assessed.

If you handle data from customers or third parties, being prepared for investigative measures with an appropriate procedure plan is a matter of compliance. Compliance with the law here means avoiding claims for damages as a result of unauthorized handover of data or a (system) outage as a result of investigative measures.

If, as a provider, you handle the data of a range of customers, you must handle these separately. This is already an obligation under data protection law, which results from § 9 of the German Data Protection Act (BDSG) together with the annex to § 9 BDSG (separation requirement). Under the GDPR, there is no lower level of protection. Virtual separation on the same hardware may be sufficient. With regard to investigative measures, for example, this must be designed in such a way that only the data of an individual customer can be viewed and isolated during an inspection in order to hand it over to the investigative authorities as a copy or image. Clarify contractually with the customer what is acceptable and what is not.

However, you should also have separated the data so that the handover or access of the investigative authorities to the relevant data is limited. If you must indeed anticipate seizures, then the data should be apportioned to different hardware so that the investigative authorities can take only the data of the relevant customer or contractor with them. Especially if the content is “to be taken out of circulation” because it is itself subject to incrimination (e.g. content prohibited under criminal law or infringements of industrial property rights), the investigative authorities will not agree to a copy of the data or an image.

### 9.2 Test run absolutely necessary

As part of the preparation, you will always need a well-rehearsed organizational plan for the specific emergency at hand. In IT security, even the best emergency power supply is of no use if it does not start up in an emergency and cannot be serviced. It is essential that you clarify the responsibilities within the company in the event of a search.

As is usual in the IT security sector, the procedure must be tested concretely, because here, too, the real problems only become apparent during the test.

View the investigative measures – in particular the search and seizure – as a legal circumvention of the IT security measures in the company. Because IT security might be as good as possible from a technical point of view, but the investigative authority can still legally access the evidence. Here too, as everywhere in IT security, the following applies: Plan - Do - Check - Act. Preparation saves on costs!

### 9.3 Important parameters

The most important parameters and responsibilities to be defined in a process description for the search scenario are:

- Who has to inform whom (think in terms of management, defense lawyer, attorney, ...)?
- Who will be responsible for receiving the officials and, without impinging on business operations, will escort them to a separate room?
- Who on the part of the company will coordinate the communication with the leading investigating officer and the company lawyers who have arrived on site?
- Who is responsible for attending to the investigating officers in-house and recording the procedures chosen with or by the officials?
- To what extent may employees cooperate – and where do the limits lie? Be precise and restrictive about what you allow so that employees do not have any decision-making leeway. Brief them on these accordingly.
- What information is permitted? Provide clear service/work instructions that the questioning of witnesses is not permitted on the business premises.
- Who in the company has the right to object to the seizure of data or objects so that this is confined to a sovereign act of seizure?
- Who ensures that the seizure inventory is complete and officially accepts it?
- Who prepares a report on the course of the search in consultation with all employees involved?

## 10 Dealing with “Requests to Preserve Evidence” by Law Enforcement Authorities

In principle, there is no obligation for private individuals or private companies to participate in or actively support investigations and investigative measures by law enforcement authorities. However, the following must be borne in mind: Anyone who destroys/deletes data that can be used for evidentiary purposes in investigative proceedings may become liable to prosecution because of obstruction of justice (§ 258 StGB – German Penal code), for example.

It will also get complicated if employees or persons in charge of the company have knowledge of data with criminal content or know that stored data may be relevant for an investigatory procedure. If this knowledge arises as a result of the investigative authorities approaching the company, this data must be stored in keeping with the legal obligations arising from the provisions of the Telecommunications Act (TKG) and the Telemedia Act (TMG) and preferably saved on external data carriers. Just as with a request for information by the investigative authorities, here it also applies that you can insist that the investigative authorities provide such a “preservation of evidence request” in writing, and stating the legal basis. Under no circumstances should any rash or premature action be taken and further data be stored or even handed over in response to the “first call” of the police or the public prosecutor’s office, with the exception of existing obligations under the Telecommunications Act (TKG §§ 113, 95, 111) and Telemedia Act (TMG). Otherwise, this could lead to administrative offenses or even criminal offenses being committed due to violations of data protection regulations, among other things.

Ultimately, it can therefore be asserted that outside the obligations under the Telecommunications Act (TKG §§ 95 and 111) in conjunction with § 100j of the German Criminal Code (StPO), there is no obligation whatsoever to comply with a request by the investigative authorities to preserve evidence. Naturally, in order to prevent a greater investment of time and expense or further investigation and compulsory measures down the line, de-escalation must be considered and, within the scope of what is legally permissible, a calm and proportionate reaction must be adopted. In cases of doubt, a specialist lawyer in criminal law should always be consulted.

## 11 Knowledge of Criminally-Relevant Information

How should you react if you discover or are made aware of potentially criminally-relevant information?

### 11.1 Check duty of disclosure

In this context, it should first be made clear that private persons and private companies are only obliged to report the criminal offenses explicitly ment-

ioned in § 138 StGB (German Penal Code). The criminal offenses cited there are serious crimes involving endangering peace or high treason, offenses that endanger the state or terrorism, murder and manslaughter, offenses against personal liberty, robbery, extortion under threat of force, and offenses creating a danger to the public such as arson.

This duty to report planned and/or already committed criminal offenses is specified in § 138 of the German Penal Code (StGB). There is no further obligation to report criminal offenses. If you are unsure whether such an obligation to report exists, you should also consult a specialist lawyer for criminal law.

Furthermore, in certain cases there is an obligation to report suspicious cases, for example pursuant to § 11 (1) of the Money Laundering Act. Here, too, failure to report can constitute a misdemeanor punishable with fines.

Outside these legally regulated cases, there is no criminal offense of “complicity”. However, employees of the company could end up being suspected of aiding and abetting another person to commit a criminal offense. Due to a lack of intent, this will regularly be ruled out, but it cannot be ruled out that the law enforcement authorities will initiate investigative proceedings. It is therefore important to take precautions and to address and clarify any suspicious factors as early as possible.

### 11.2 Establishing codes of conduct

It goes without saying that neither you nor your company want to act as “accomplices” to criminals. You should make this clear in corresponding provisions in your general terms and conditions and emphasize that the use of your services to perpetuate criminal offenses is prohibited and will lead to termination of the contractual relationship as well as to criminal charges.

In order not to end up being suspected of criminal action yourself, you should cooperate with the investigative authorities and, if you are aware of justified suspicious cases, secure the corresponding data as evidence – that is, document when, what, by whom, based on what circumstances, and with what content the data was secured. In addition, you should terminate the business relationship and simultaneously inform the law enforcement authorities. This procedure should also be implemented as part of a transparent compliance system with concrete codes of conduct for all employees.

### 11.3 eco Complaints Office – Options for reporting to non-police body

The eco Complaints Office has been fighting illegal content in the Internet for over 15 years. It is embedded in the system of regulated self-regulation and has, in particular, the task of improving youth protection in the Internet.

Internet users who come across illegal and – in particular – youth-endangering content, or Internet Service Providers (ISPs) who find such content on their own servers, can make a free and anonymous report under <https://international.eco.de/internet-complaints-office.html>, <https://www.internet-beschwerdestelle.de/en/index.html> or by email to [hotline@eco.de](mailto:hotline@eco.de). Such criminally relevant content includes, for example:

- youth-endangering and development-impairing content,
- freely accessible adult pornography, pornography depicting violence, animals, children, or juveniles,
- the production or provision of naked images of minors for profit,
- dissemination of symbols and propaganda material of unconstitutional organizations,
- incitement of the masses,
- instructions for or incitement of criminal offenses,
- depictions of extreme violence,
- grooming, or
- unsolicited sending of advertising emails and newsletters.

The eco Complaints Office team consists of staff with legal training who start by subjecting incoming complaints to a comprehensive preliminary legal assessment. If the reported content is illegal, the police and/or the ISP will be informed, depending on the violation. In so doing, the specific content and the source of the find are clearly stated and the legal justification presented and, if applicable, reference is made to criminal charges already filed.

A simplified depiction of the processing of German cases



To effectively combat illegal Internet content, the Complaints Office cooperates with providers, partner complaints offices, and law enforcement authorities, among others. In addition, eco is a founding member of the international network of complaint offices (INHOPE) and part of the German Safer Internet Center. These collaborations help to attain the rapid removal of content at its source, so that it cannot be seen by any other person, and to ensure effective criminal prosecution, thus holding perpetrators accountable. The eco Complaints Office also supports the law enforcement authorities and ISPs through opportunities for exchanging experiences and ideas and training actions (especially in the area of youth media protection), through policy-making, and through dealing with reports on illegal content.

## Authors

Attorney-at-Law Dr. Jens Eckhardt

*Law firm Derra, Meyer & Partner Attorneys-at-Law, Dusseldorf, Ulm, Berlin  
Specialist Lawyer in IT Law  
Privacy Auditor (TÜV)  
Compliance Officer (TÜV)  
Member of the executive board of EuroCloud Deutschland\_eco e.V.*



Since 2001, Dr. Jens Eckhardt has been practising law in the fields of privacy, IT, telecommunications, and marketing. His doctorate was on the topic of telecommunications surveillance. He provides consultancy advice to national and international companies in these fields – both in terms of strategy (in particular with regard to outsourcing, the introduction of new systems, processes, technologies, as well as marketing strategies and technologies) and case-related (in particular concerning inquiries by regulatory authorities, legal disputes, and individual questions).

Attorney-at-Law Konrad Menz

*Law firm Derra, Meyer & Partner Attorneys-at-Law, Ulm, Stuttgart*

*Specialist Lawyer in Criminal Law*

*Specialist Lawyer in Tax Law*

*Specialist Lawyer in Insolvency Law*

*Compliance Officer (TÜV)*



Konrad Menz represents clients in all areas of commercial criminal law. With his specialist knowledge, he also supports companies through risk and preventive consultancy advice. Here he combines many years of practical experience in criminal, tax, and insolvency law in order to establish and evaluate practice-oriented compliance structures.

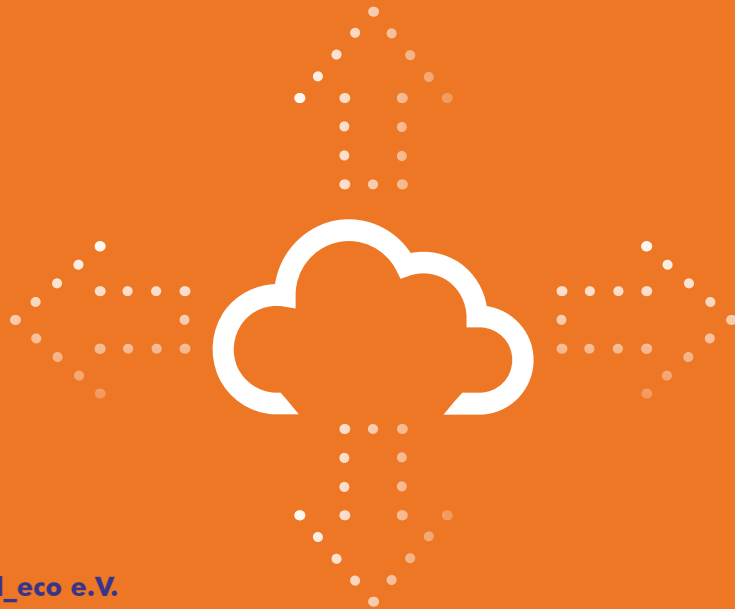
Attorney-at-Law Ralph E. Walker

*Law firm Derra, Meyer & Partner Attorneys-at-Law, Ulm, Augsburg*

*Specialist Lawyer in Criminal Law*



Ralph E. Walker exclusively handles criminal briefs. Since the very outset of his professional career, he has concentrated and specialized wholly on work as a criminal defense lawyer. Attorney Walker defends cases throughout Germany, with a focus on commercial and insolvency criminal law. Thanks not only to his many years of experience as a criminal defense attorney appearing before local and regional courts, but also to his representation before the State Security Senate of the Higher Regional Courts of Munich and Stuttgart, Ralph E. Walker has gained outstanding knowledge of criminal procedural law.



**EuroCloud Deutschland\_eco e.V.**

Lichtstrasse 43h

50825 Cologne

Germany

Phone: +49 221 / 70 00 48 – 0

Fax: +49 221 / 70 00 48 – 111

email: [info@eurocloud.de](mailto:info@eurocloud.de)

Web: [www.eurocloud.de](http://www.eurocloud.de)