Scout24 Data Protection Code of Conduct

Preamble

Dear Scouts,

Data protection is a topic affecting every one of us – by handling personal data of our customers and users or as an employee whose data are being processed. As the leading operator of digital market places in Germany and Europe, Scout24 has a particular responsibility to ensure the best data protection possible for its employees, customers and users.

The objective of data protection is protecting individuals against his/her right to privacy being impaired in handling their personal data. Anyone has the right to control the disclosure and use of his or her personal data him-/herself.

This requires acting responsibly in handling personal data but also risk-conscious use of IT systems and applications.

Data protection legislation, in particular the EU General Data Protection Regulation (GDPR), sets the legal rules for collecting, processing and using personal data of employees, customers, service providers or other third parties on the basis of legal provisions only. The legal obligation to preserve data privacy applies for all employees during and even after termination of their employer-employee relationship.

Tobias Hartmann
CEO

Dirk Schmelzer
CFO

Contents

Why is this Data Protection Code of Conduct necessary?

Protecting the informational self-determination and privacy and the security of data processing are key concerns for the Scout24 Group and an important requirement for the trust of our employees, customers and users in us.

All regulations must be compliant with the provisions of the General Data Protection Regulation, the German Federal Data Protection Act and all field-specific standards for data protection. In addition, Scout24 commits to compliance with the principles of transparency, necessity of the processed data and data minimisation to the utmost extent.

The protection of customer and employee data has the highest priority.

Our data protection concept

The Scout24 Group is active in various European countries, and handling customer data is a material part of the Scout24 Group activities. The users of our platforms do not only trust us with their data required for registration but also with information about their personal circumstances.

Our goal is to justify our customers' trust in the security on our platforms.

The protection of customer and employee data has the highest priority. Therefore, compliance with data protection and data safety are an integral part of our self-image as the Scout24 Group.

Responsibility

Data protection compliance is originally a responsibility of the board of directors and the management and thereby a part of corporate accountability in management. At Scout24, we have established a data protection unit in which certain data protection obligations are delegated and which is therefore assigning the responsibility for compliance with the requirements under data protection law to the operational departments, market segments and entities.

The data protection controllers make binding decisions for data protection in their field for the respective market segments, entities and companies of the Scout24 Group. They are supported in this by the data co-ordinators to whom the data protection controllers may also delegate individual tasks associated with compliance with the requirements under data protection law.

In addition, data protection officers are appointed in the Scout24 companies who inform and advise us on issues under data protection law, review compliance with the provisions under data protection law and support data subjects in exerting their data protection rights and providing transparency in data processing.

Notwithstanding the above, data protection compliance is a common task of all Scout24 Group employees for us. We enable data protection-compliant activities by processing personal data within the scope of our authority exclusively and in line with the instructions of the respective person responsible. We support the data protection controllers and data co-ordinators in performing their function. We keep up-to-date about changes in our area of work relevant for data protection.

What does this mean for me?

- Internalise the data protection guidance you receive upon joining Scout24 and during your work for us.
- Be mindful of complying with the data protection policy and the supporting procedures.
- Familiarise yourself with the applicable data protection provisions and take part in data protection training relevant for you.
- If you have any doubts whether your actions are compliant with data protection requirements, contact the responsible person in the data protection unit.

Legitimacy, processing in good faith, transparency

Handling of personal data is subject to strict legal provisions. The EU General Data Protection Regulation (GDPR) effective as of May 2018 provides strict requirements for collecting and processing such data. Any breach can be sanctioned with high fines of up to EUR20 million or 4% of the company's global revenue. We are considering this legal framework in all of our decisions.

We are only processing personal data in a legitimate way in good faith (honestly and ethically) and in a manner comprehensible to our customers, employees and other data subjects.

In doing so, we show consideration for the fact that on principle, processing of personal data is prohibited by law and we need an authorisation for their processing in the individual case. Such authorisation is deemed granted if either the data subject has effectively consented to the specific data processing or a legal provision allows for such data processing. Therefore, we are reviewing all instances of processing of personal data in advance to check whether such authorisation is present.

In addition, we are considering the principle of fairness in each instance of data processing. The data subjects should be enabled to learn of any processing affecting them. For such purpose, we are advising them properly and comprehensively about the circumstances of collection and use of their data. We are arranging this information in such a way that it is easily accessible and comprehensible and written in clear and simple language.

What does this mean for me?

- Document all intended instances of processing personal data for which you are responsible in the directory for processing activities.
- In case of doubt, consult the legal department.

When in doubt: Consult!

Use for the intended purpose

A material principle of personal data processing is their use for the intended purpose. Therefore, we are collecting personal data for defined, clear and legitimate purposes only and do not process them in any manner not reconcilable with such purposes. In this regard, it is crucial to identify the purpose for which the data are collected and processed even before collecting them. The purpose determines e.g. for what the data can be used and for how long they may be stored.

It is also possible to define several purposes; however, it must be ensured that each purpose is defined with sufficient finality and is not described too generally. This includes but is not limited to us abstaining from data collection “just in case”.

We also ensure that the purpose of collection is legitimate. This means that there is an effective legal basis (e.g. processing for fulfilment of a contract or rendering of specific services) and that processing does not constitute a breach of other applicable legal standards.

We check very carefully whether we can use data for other purposes than the original purposes of collection. Usually, we only may do so if the new purpose is consistent with the original purpose, e.g. if it is a logical consequence of the initial data processing.

What does this mean for me?

- Before a planned data collection, think about for what the data are specifically needed.
- Do not collect any data “just in case”, i.e. without a specific purpose being present for the use of data.
- Ensure that the data collection and its purposes are recorded accurately and completely in the directory of processing activities.
- Be careful when changing the processing purpose retroactively. Check carefully in each case whether the purpose is compatible and there is a sufficient legal basis for the additional processing. In case of doubt, consult your data co-ordinator or the legal department.

Data minimisation

Data are part of our business model. Thus, we depend on collecting and using data. However, with regard to personal data, collection and use may not be without reason.

Therefore, we take care that the personal data collected and processed by us are appropriate for the purpose and significant and are limited to the extent required for the purpose of processing.

For this, we ensure that the data collected have adequate relevance for the purpose of processing and are suitable for its promotion. The quantity of data collected should be held as low as possible. If the purpose of processing can be achieved in the same manner and the same quality when using anonymous data, we will anonymise the data before processing them further. On principle, we give priority to use of anonymised data.

What does this mean for me?

- Do not collect any data “just in case”, i.e. without a specific purpose being present for the use of data.
- Before collecting personal data, check whether the purpose may be achieved just as well using anonymous data.
- When collecting data, also take into consideration the technical implementation; only indicate required fields if the data are essential.

Accuracy of data

We take care that the personal data we are processing are factually accurate and up to date if required with regard to the respective purpose of processing. This means that we assure that the information assigned to individual persons by us is factual as provided by the respective purpose of processing.

We take all required steps to immediately correct or erase inaccurate personal data. This means that we correct or erase the data as soon as we become aware of their inaccuracy. Likewise, we will comply with corresponding requests of the data subjects.

What does this mean for me?

- Take care that the data collected and processed under your responsibility are accurate.
- Arrange for rectification of inaccurate personal data as soon as you become aware of their inaccuracy.
- Ensure that any such requests of the data subjects for rectification or erasure of inaccurate data are processed according to the requirements of data protection law (take into account the procedure for rights of data subjects) and contact your data co-ordinator or the legal department in case of doubt.

Limitation of storage

Frequently, we are interested in storing data about our customers, users and other data subjects in the long term, for example within the scope of long-standing contractual relationships or also in compliance with legal duties to retain records. In doing so, we may not lose sight of the fact that our interest in storing such data must always be justified and serve the purpose previously established. Processing of personal data is subject to time limits.

On principle, we are storing personal data enabling identification of the data subjects only for as long as required for the purposes for which they are processed. To enable this, we are establishing time limits for their erasure or at least for regular review of data when collecting such data.

If we do not need the data any longer, we ensure that the data are erased or anonymised. In those cases, we also comply with appropriate requests for erasure by the data subject.

Processing of personal data is subject to time limits.

What does this mean for me?

- Take care that the data collected and processed under your responsibility are stored only for as long as necessary for achieving the specifically pursued purpose.
- Already define specific maximum time limits when collecting the data and make note of them in the directory for processing activities.
- Ensure that corresponding requests for erasure of data that is no longer needed by the data subjects are processed according to the requirements under data protection law (procedure for rights of data subjects) and contact your data co-ordinator or the legal department in case of doubt.

Integrity and confidentiality

Data security is one of the great challenges of our time. As the operator of large market networks, we have a special responsibility to ensure the best possible security for the data of our employees, customers and users.

Therefore, we ensure that personal data is processed in a way providing appropriate protection against unauthorised or illegitimate processing and unintentional loss, unintentional erasure or unintentional damage. For such purpose, we take appropriate technical and organisational measures.

To guarantee a level of protection appropriate for the risk of processing, we are aligning the type and extent of these measures with (1) the state of the art, (2) the costs of implementation, (3), nature, extent, circumstances and purposes of data processing and (4) the probability and severity of the risk.

What does this mean for me?

- Take care to provide sufficient data security measures in consideration of the respective classification of the information.
- Ensure that the data security measures for the processing procedures you are responsible for are documented in the directory of processing activities.
- If using data processing service providers, take care to bind them to compliance with sufficient security measures.

If you become aware of breaches of data security, including events of destruction, loss, change or unauthorised disclosure of personal data, report them immediately upon becoming aware of them according to the crisis management & crisis communication policy applicable for Scout24 or by means of the external compliance hotline:

Dr. Rainer Frank
Fachanwälte für Strafrecht
(Specialists for criminal law)
am Potsdamer Platz

+49 30 31 86 85-79
compliance-scout24@fs-pp.de
www.compliance-scout24.fs-pp.de

Where can you find help?

You can find further contacts in the area of data protection or from the crisis management team on the Compass page under “Data protection”.

Contact data protection officer:
Simone Rosenthal
ISiCO Data Protection GmbH
External Data Protection Officer of the Scout24 Group
info@isico-datenschutz.de
Tel:. +49 30-213 00 28 50

If you wish to exchange confidential information, please first use this e-mail address to contact the data protection officer directly.

Scout24 AG
c/o ImmobilienScout24 GmbH
Invalidenstraße 65
10557 Berlin

riskcompliance@scout24.com