Privacy Policy

The MyIFCO WebClearing platform

Last updated: March 2022

Table of contents

I. Name and address data controller

In terms of the EU General Data Protection Regulation and other national data protection laws of the Member States and other data protection regulations, the Data Controller is:

IFCO SYSTEMS GmbH
Zugspitzstraße 7
82049 Pullach
Germany
+49 89 744 91 0
info@ifco.com
www.ifco-online.com

II. Contact details data protection officer

The Data Protection Officer for the Data Controller is:

DataCo GmbH
Dachauer Straße 65
80335 Munich
Germany
+49 89 7400 45840
www.dataguard.de

III. Data subject rights

When your personal data is processed, you are a data subject within the meaning of the GDPR and have the following rights:

1. Right to information

You may request the data controller to confirm whether your personal data is processed by them. If such processing occurs, you can request the following information from the data controller:

- The purpose for which the personal data is processed.
- The categories of personal data being processed.
- The recipients or categories of recipients to whom the personal data have been or will be disclosed.
- The planned duration of the storage of your personal data or, if specific information is not available, criteria for determining the duration of storage.
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing.
- The existence of the right to lodge a complaint with a supervisory authority.
- Where personal data are not collected from you any available information as to their source.
- The existence of automated decision-making including profiling under Article 22 (1) and Article 22 (4) GDPR and, in certain cases, meaningful information about the data processing system involved, and the scope and intended result of such processing on the data subject.

You have the right to request information on whether your personal data will be transmitted to a third country or an international organization. In this context, you can then request the appropriate guarantees in accordance with Art. 46 GDPR in connection with the transfer.

Your right to information may be limited where it is likely that such restriction will render impossible or seriously impede the achievement of scientific or statistical purposes and that such limitation is necessary for the achievement of scientific or statistical purposes.

2. Right to rectification

You have a right to rectification and/or modification of the data if your processed personal data is incorrect or incomplete. The data controller must correct the data without delay.

Your right to rectification may be limited to the extent that it is likely to render impossible or seriously impair the achievement of the purposes of the research or statistical work and the limitation is necessary for the achievement of the purposes of the research or statistical work.

3. Right to the restriction of processing

You may request the restriction of the processing of your personal data under the following conditions:

- If you challenge the accuracy of your personal data for a period that enables the data controller to verify the accuracy of your personal data.
- The processing is unlawful, and you oppose the erasure of the personal data and instead request the restriction of their use instead.
- The data controller or its representative no longer need the personal data for the purpose of processing, but you need it to assert, exercise or defend legal claims; or
- If you have objected to the processing pursuant to Art. 21 (1) GDPR and it is not yet certain whether the legitimate interests of the data controller override your interests.

If the processing of personal data concerning you has been restricted, this data may – with the exception of data storage – only be used with your consent or for the purpose of asserting, exercising

or defending legal claims or protecting the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

If the processing has been restricted according to the aforementioned conditions, you will be informed by the data controller before the restriction is lifted.

Your right to restrict the processing may be limited where it is likely that such restriction will render impossible or seriously impede the achievement of scientific or statistical purposes and that such limitation is necessary for the achievement of scientific or statistical purposes.

4. Right to erasure

a) Obligation to erase

If you request from the data controller to delete your personal data without undue delay, they are required to do so immediately if one of the following applies:

- Personal data concerning you is no longer necessary for the purposes for which they were collected or processed.
- You withdraw your consent on which the processing is based pursuant to Art. 6 (1) (1) (a) and Art. 9 (2) (a) GDPR and where there is no other legal basis for processing the data.
- According to Art. 21 (1) GDPR you object to the processing of the data and there are no longer overriding legitimate grounds for processing, or you object pursuant to Art. 21 (2) GDPR.
- Your personal data has been processed unlawfully.
- The personal data must be deleted to comply with a legal obligation in Union law or Member State law to which the data controller is subject.
- Your personal data was collected in relation to information society services offered pursuant to Art. 8 (1) GDPR.

b) Information to third parties

If the data controller has made your personal data public and must delete the data pursuant to Art. 17 (1) GDPR, they shall take appropriate measures, including technical means, to inform data processors who process the personal data, that a request has been made to delete all links to such personal data or copies or replications of the personal data, taking into account available technology and implementation costs to execute the process.

c) Exceptions

The right to deletion does not exist if the processing is necessary

- to exercise the right to freedom of speech and information;
- to fulfil a legal obligation required by the law of the Union or Member States to which the data controller is subject, or to perform a task of public interest or in the exercise of public authority delegated to the representative.
- for reasons of public interest in the field of public health pursuant to Art. 9 (2) (h) and Art. 9 (2) (i) and Art. 9 (3) GDPR.
- for archival purposes of public interest, scientific or historical research purposes or for statistical purposes pursuant to Art. 89 (1) GDPR, to the extent that the law referred to in subparagraph (a) is likely to render impossible or seriously affect the achievement of the objectives of that processing, or
- to enforce, exercise or defend legal claims.

5. Right to information

If you have the right of rectification, erasure or restriction of processing over the data controller, they are obliged to notify all recipients to whom your personal data have been disclosed of the correction

or erasure of the data or restriction of processing, unless this proves to be impossible or involves a disproportionate effort.

You reserve the right to be informed about the recipients of your data by the data controller.

6. Right to data portability

You have the right to receive your personal data given to the data controller in a structured and machine-readable format. In addition, you have the right to transfer this data to another person without hindrance by the data controller who was initially given the data, if:

- the processing is based on consent in accordance with Art. 6 (1) (1) (a) GDPR or Art. 9 (2) (a) GDPR or performance of a contract in accordance with Art. 6 (1) (1) (b) GDPR and
- the processing is done by automated means.

In exercising this right, you also have the right to transmit your personal data directly from one person to another, insofar as this is technically feasible. Freedoms and rights of other persons shall not be affected.

The right to data portability does not apply to the processing of personal data necessary for the performance of a task in the public interest or in the exercise of official authority delegated to the data controller.

7. Right to object

For reasons that arise from your particular situation, you have, at any time, the right to object to the processing of your personal data pursuant to Art. 6 (1) (1) (e) or 6 (1) (1) (f) GDPR; this also applies to profiling based on these provisions.

The data controller will no longer process the personal data concerning you unless he can demonstrate compelling legitimate grounds for processing that outweigh your interests, rights and freedoms, or the processing is for the purpose of enforcing, exercising or defending legal claims.

If the personal data relating to you are processed for direct marketing purposes, you have the right to object at any time to the processing of your personal data in regard to such advertising; this also applies to profiling associated with direct marketing.

If you object to processing for direct marketing purposes, your personal data will no longer be processed for these purposes.

Regardless of Directive 2002/58/EG, you have the option, in the context of the use of information society services, to exercise your right to object to automated decisions that use technical specifications.

You also have the right to object, on grounds relating to your particular situation, to the processing of personal data concerning you which is carried out for scientific or historical research purposes or for statistical purposes pursuant to Article 89 (1) of the GDPR.

Your right to objection may be limited where it is likely that such restriction will render impossible or seriously impede the achievement of scientific or statistical purposes and that such limitation is necessary for the achievement of scientific or statistical purposes.

8. Right to withdraw the data protection consent declaration

You have the right to withdraw your consent at any time. The withdrawal of consent does not affect the legality of the processing carried out on the basis of the consent until the withdrawal.

9. Automated decisions on a case-by-case basis, including profiling

You have the right to not be subject to a decision based solely on automated processing – including profiling – that will have a legal effect or substantially affect you in a similar manner. This does not apply if the decision:

- is required for the conclusion or execution of a contract between you and the data controller,
- is permitted by the Union or Member State legislation to which the data controller is subject, and where such legislation contains appropriate measures to safeguard your rights and freedoms and legitimate interests, or
- is based on your explicit consent.

However, these decisions must not be based on special categories of personal data under Art. 9 (1) GDPR, unless Art. 9 (2) (a) or Art. 9 (2) (b) GDPR applies and reasonable measures have been taken to protect your rights and freedoms as well as your legitimate interests.

With regard to the cases referred to in (1) and (3), the data controller shall take appropriate measures to uphold your rights and freedoms as well as your legitimate interests, including the right to obtain assistance from the data controller or his representative, to express your opinion on the matter, and to contest the decision.

10. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, you shall have the right to complain to a supervisory authority, in the Member State of your residence, or your place of work or place of alleged infringement, if you believe that the processing of the personal data concerning you violates the GDPR.

The supervisory authority to which the complaint has been submitted shall inform the complainant of the status and results of the complaint, including the possibility of a judicial remedy pursuant to Art. 78 GDPR.

The supervisory authority responsible for IFCO Systems GmbH is

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach
Deutschland
Phone: +49 (0) 981 180093-0
E-Mail: poststelle@lda.bayern.de
www.lda.bayern.de

IV. Data processing on the MyIFCO WebClearing platform

1. Description and scope of data processing

On this page we inform you about the privacy policy applicable for the MyIFCO WebClearing platform ("platform" or “MyIFCO”). The platform is an offer of IFCO SYSTEMS GmbH, Zugspitzstraße 7, 82049 Pullach, Germany ("IFCO SYSTEMS GmbH ", "we" or "us").

Other information about our data protection can be found in the privacy policy of our website: https://www.ifco.com/privacy-notice/

The MyIFCO WebClearing Platform facilitates the web-based planning, control, and management of returnable plastic crates (RPCs). The platform allows customers to conduct their transactions

electronically and view the inventory and RPC movements in real time.
The transactions are synchronised between the head office and the branches fully automatically. User account permissions and all local settings can also be controlled over the platform.

The following data is processed here:

- Email address
- First name
- Second name
- Password
- Username
- IFCO No.
- User ID
- Last login time
- Browser used
- Date of changes to users (e.g., setup date)

This data is recorded when the user account is setup. User accounts are setup by IFCO employees or authorised IFCO customer employees. The customer transfers the data himself on a customer data sheet by email or fax.

Actions are also logged, i.e., when a user performs a specific transaction, such as booking a movement.

Please note, that the MyIFCO order portal is based on the e-business and e-commerce platform jStage from iSYS Software GmbH, Grillparzerstr. 10, 81675 Munich, Germany.

2. Purpose of data processing

Processing personal data serves to create a user, and to identify, set permissions for and grant the user access to the MyIFCO WebClearing Platform and to provide the requested service.

Users can also contact Customer Service over the MyIFCO WebClearing Platform, for example, to have their password reset.

3. Legal basis for data processing

As for the processing of personal data required for the performance of a contract of which the data subject is party, Art. 6 (1) (1) (b) GDPR serves as the legal basis. This also applies to processing operations required to carry out pre-contractual activities.

4. External recipients of personal data

Depending on which modules are used by MyIFCO, different processors may be recipients of personal data if they take over a partial service of the processing process. Categories of recipients of personal data are in particular:

- Hosting service providers
- IT service providers for maintenance, security, and support purposes
- Other processors contracted to provide and improve our platform

If recipients of personal data are located outside the EU or the EEA, IFCO SYSTEMS GmbH actively creates suitable guarantees for legally compliant data transfer to third countries. To ensure appropriate guarantees for the protection of the transfer and processing of personal data outside the EU, the transfer of data to and processing of data by Microsoft is protected by appropriate guarantees pursuant to Art. 46 et seq. GDPR, in particular by concluding so-called standard contractual clauses pursuant to Art. 46 (2) (c) GDPR. A copy of the appropriate guarantees can be requested by sending us an email at the above-mentioned contact information.

4. Period of storage

Your personal information is stored for as long as required to fulfil the aims described in this Privacy Policy or as required by law.

This is the case when the user is inactive for 2 years, after which the email address is deleted.

5. Objection and erasure

Further information on objection and erasure options against IFCO can be found at: https://www.ifco.com/de/en/privacy-notice/05eb382dce424e4b

V. Platform staging and log file creation

1. Description and scope of data processing

The platform and its databases are hosted on servers that belong to the service provider:

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA
425 882 8080
http://www.microsoft.com

The servers automatically collect and store information in what are referred to as server log files that your browser automatically transfers when you visit our platform. The information stored comprises:

- Browser type/Browser version
- Operating system used
- Referring URL
- The host name of the computer accessing our platform
- Date and time of the server request
- IP address

This data is not merged with other data sources. Third parties do not receive access to server log files.

Telemetry data is also processed for the following purposes:

- Infrastructure monitoring
- Application monitoring
- Resource optimisation
- Troubleshooting
- Protocol analysis

The Microsoft Azure servers of the platform are geographically located in the European Union (EU), in Amsterdam and Dublin respectively. The data processed is encrypted in order to only allow authorized access. Nevertheless, it cannot be excluded that data will be processed in the United States of America. The European Union does not consider that the US provides an adequate level of data protection. To ensure appropriate guarantees for the protection of the transfer and processing of personal data outside the EU, the transfer of data to and processing of data by Microsoft is protected by appropriate guarantees pursuant to Art. 46 et seq. GDPR, in particular by concluding so-called standard contractual clauses pursuant to Art. 46 (2) (c) GDPR. A copy of the appropriate guarantees can be requested by sending us an email at the above-mentioned contact information.

2. Purpose of data processing

The temporary storage of the IP address by the system is necessary for the delivery of the platform to the computer of the user. For this purpose, the user's IP address must be kept for the duration of the session.

Storage in log files takes place to ensure the functionality of the platform. The data is also used to optimise the platform and safeguard the security of our information technology systems. An evaluation of the data for marketing purposes does not take place in this context.

For the aforementioned purposes, our legitimate interest lies in the processing of data in compliance with Art. 6 (1) (1) (f) GDPR.

3. Legal basis for data processing

The storage of server log files takes place subject to Art. 6 (1) (1) (f) GDPR. The platform operator has a legitimate interest in presenting and optimising their platform in a manner that is free of technical errors, for which purpose the server log files need to be collected.

4. Duration of storage

The data is deleted as soon as it is no longer required for the purpose it was collected. The collection of data for staging the platform takes place once the respective session is completed.

If the data is stored in log files, this is the case after seven days at the latest. Storage beyond this is possible. In this case, the IP addresses of the users are deleted or anonymised so that an assignment of the calling client is not possible.

5. Objection and erasure

Collection of the data for the purpose of serving our platform and storing the data in log files is essential for operating our platform. This means that there is no option available to object on the part of the user.

VI. Use of cookies

1. Description and scope of data processing

Our platform uses cookies. Cookies are text files that are stored in or by the Internet browser on the user's computer system. When a user accesses a platform, it allows a cookie to be stored on the user's operating system. This cookie contains a characteristic string that allows for the unique identification of the browser when the platform is accessed again.

We use cookies to make our platform more user-friendly. Some elements of our platform require identification of the accessing browser even after a change in page.

The following data is stored and transferred in these cookies:

- Generic ID in a sticky session cookie/session cookie
- Language settings

We also use cookies on our website, which enable us to analyse the browsing behaviour of our users. As a result, the following data will be transmitted:

- Entered search queries
- Frequency of page views
- Use of website functionalities

The user data collected in this manner is pseudonymised by technical measures. It is therefore not possible to assign the data to the user accessing the platform. The data is not stored together with other personal data of the users.

2. Purpose of data processing

The purpose of using technical cookies is to simplify the use of our platform for users. Some functions of our platform cannot be offered without the use of cookies. These require that the browser is recognized even after a page change.

We require cookies for the following applications:

- Log-in information from the user over sticky session cookies/session cookies
- Storing the language setting

The user data collected by technical cookies are not used to create user profiles.
The analysis cookies are used for the purpose of improving the quality of our platform and its content. Through the analysis cookies, we learn how the platform is used and thus can constantly optimize our offer.

3. Legal basis for data processing

Legal basis for processing of personal data using non-technical cookies is Art. 6 (1) (1) (a) GDPR.

Legal basis for processing of personal data using technical cookies is Art. 6 (1) (1) (f) GDPR.

4. Duration of storage, objection and erasure

Cookies are stored on the user's device and transmitted to our site by the user. Therefore, you as a user also have full control over the use of cookies. You can deactivate or restrict the transmission of cookies by changing the settings in your internet browser. Cookies that have already been saved can

be deleted at any time. This can also be done automatically. If cookies are deactivated for our platform, it is possible that not all functions of the platform can be used to their full extent.

If you use the Safari browser version 12.1 or higher, cookies will be automatically deleted after seven days. This also applies to opt-out cookies, which are used to prevent the use of tracking mechanisms.

VII. Contact via email

1. Description and scope of data processing

You can contact us via the email address provided on our platform. In this case the personal data of the user transmitted with the email will be stored.

After a successful request, your personal data will be processed in our ticketing system Jira of Atlassian Corporation Plc, 341 George Street Level 6, Sydney, NSW 2000, Australia (hereinafter referred to as: Atlassian). In the process, the data may be transferred to Atlassian's servers in Australia. Part of the data processing agreement with Atlassian are so-called EU standard contractual clauses pursuant to Art. 46 (2) (c) GDPR. These are classified as appropriate guarantees for the protection of the transfer and processing of personal data outside the EU. In addition to the standard contractual clauses, technical and organisational measures are in place to ensure and guarantee an appropriate and adequate level of data protection. A copy of the standard contractual clauses can be requested by sending us an informal email.

For more information about Atlassian's processing of data, please click here: https://www.atlassian.com/legal/privacy-policy

The data will be used exclusively for the processing of the conversation.

2. Purpose of data processing

If you contact us via email, this also constitutes the necessary legitimate interest in the processing of the data.

3. Legal basis for data processing

The legal basis for the processing of data transmitted while sending an email is Art. 6 (1) (1) (f) GDPR. If the purpose of the email contact is to conclude a contract, the additional legal basis for the processing is Art. 6 (1) (1) (b) GDPR.

4. Duration of storage

The data will be deleted as soon as it is no longer necessary to achieve the purpose for which it was collected. For personal data sent by email, this is the case when the respective conversation with the user has ended. The conversation ends when it can be concluded from the circumstances that the matter in question has been conclusively resolved.

5. Objection and erasure

The user has the possibility to withdraw the consent to the processing of their personal data at any time. If the user contacts us by email to info@ifco.com, he can object to the storage of his personal data at any time.

In this case, all personal data stored while establishing contact will be deleted.

VIII. Contact form

1. Description and scope of data processing

A contact form is available on our platform which can be used to establish electronic contact. Only already registered users of the MyIFCO WebClearing Platform can use this contact option.

After a successful request, your personal data will be processed in our ticketing system Jira of Atlassian Corporation Plc, 341 George Street Level 6, Sydney, NSW 2000, Australia (hereinafter referred to as: Atlassian). In the process, the data may be transferred to Atlassian's servers in Australia. For more information about Atlassian's processing of data, please see VII.2 and/or click here: https://www.atlassian.com/legal/privacy-policy

If a user uses this option, the data entered in the contact form is transferred to us and stored.
The following specific data is stored at the time the message is sent:

- IFCO no.
- Company
- Postal code
- Town
- Country
- First name
- Name
- User ID
- Customer Service responsible
- Email address
- Date and time of registration

As part of the sending process, your consent will be obtained for the processing of your data and reference will be made to this privacy policy. Alternatively, you can contact us via the email address provided. In this case the personal data of the user transmitted with the email will be stored.

The data will be used exclusively for the processing of the conversation.

2. Purpose of data processing

The processing of the personal data from the input mask serves us exclusively for the purpose of establishing contact. If you contact us by email, this also constitutes our necessary legitimate interest in the processing of the data.

The other personal data processed during the sending process serve to prevent misuse of the contact form and to ensure the security of our information technology systems.

3. Legal basis for data processing

The legal basis for the processing of the data is Art. 6 (1) (1) (a) GDPR if the user has given his consent.

The legal basis for the processing of data transmitted while sending an email is Art. 6 (1) (1) (f) GDPR. If the purpose of the email contact is to conclude a contract, the additional legal basis for the processing is Art. 6 (1) (1) (b) GDPR.

4. Duration of storage

The data will be deleted as soon as they are no longer necessary to achieve the purpose for which they were collected. For the personal data from the input mask of the contact form and those sent by email, this is the case when the respective conversation with the user has ended. The conversation ends when it can be inferred from the circumstances that the facts in question have been conclusively clarified.

5. Objection and erasure

The user has the possibility to withdraw the consent to the processing of their personal data at any time. If the user contacts us by email, he can object to the storage of his personal data. The conversation cannot be continued in this case. This option for establishing contact is only available to registered users at the moment.

In this case, all personal data stored while establishing contact will be deleted.

IX. Use of Plugins

When using our plugins and/or software, some data transfer of personal data to the US takes place. To ensure appropriate guarantees for the protection of the transfer and processing of personal data outside the EU, the transfer of data to and processing of data by corresponding processors takes place on the basis of appropriate guarantees pursuant to Art. 46 et seq. GDPR, in particular by concluding so-called standard contractual clauses pursuant to Art. 46 (2) (c) GDPR. A copy of the appropriate guarantees can be requested by sending us an informal email at the above-mentioned contact information.

We use plugins and software for various purposes. The plugins used are listed below:

Use of Mixpanel

1. Scope of processing of personal data

We use Mixpanel web analysis services of Mixpanel Inc., 405 Howard St., 2nd Floor, San Francisco, CA 94105, USA (Hereinafter referred to as Mixpanel). Mixpanel places a cookie on your computer. This allows us to store and evaluate personal data, in particular user activity (in particular which pages have been visited and which elements have been clicked on) and device and browser information (in particular the IP address and operating system). When using Mixpanel, visitor data is processed exclusively under pseudonyms.

Further information on the collection and storage of data by Mixpanel can be found here: https://mixpanel.com/privacy

2. Purpose of data processing

The use of Mixpanel serves to improve the usability and performance of our website.

3. Legal basis for the processing of personal data

The legal basis for the processing of personal data is the user's given consent in accordance with Art. 6 (1) (1) (a) GDPR.

4. Duration of storage

Your personal information will be stored for as long as is necessary to fulfil the purposes described in this Privacy Policy or as required by law, e.g. for tax and accounting purposes.

5. Possibility of withdrawal of consent and erasure

You have the right to withdraw your declaration of consent under data protection law at any time. The withdrawal of the consent does not affect the lawfulness of the processing carried out on the basis of the consent up to the withdrawal.

You can prevent the collection and processing of your personal data by Mixpanel by preventing the storage of cookies from third parties on your computer, by using the "Do Not Track" function of a supporting browser, by deactivating the execution of script code in your browser or by using a script blocker such as NoScript (https://noscript.net/) or Ghostery (https://www.ghostery.com) in your browser.

With the following link you can deactivate the use of your personal data by Mixpanel: https://help.mixpanel.com/hc/en-us/articles/360000679006-Managing-Personal-Information#optout-users

Further information on objection and erasure options against Mixpanel can be found at: https://mixpanel.com/privacy

Use of F-Secure

1. Scope of processing of personal data

We use F-Secure, a service for the detection and response to the full breadth of cyber threat actors up to including advanced persistent threats of F-Secure Cyber Security Limited, Matrix House 5th Floor,

Basing View, Basingstoke, RG21 4 DZ, a company registered in England and Wales (hereinafter referred to as F-Secure).

F-Secure leverages advanced capabilities across people, process, and technology to identify attacker Tactics, Techniques and Procedures. Initial detection of suspicious activity is achieved using 1.) automates detection (the detection rules can alert to fire when suspicious activity is detected within the data collected. Following an alert detection, F-Secure triage and investigate the suspected malicious activity in order to build additional context and filter our any false positives) and 2.) Threat Hunting (whilst the primary objective of Threat Hunting is the identification and development of detection rules it can also lead to the detection of suspicious activity).

It is possible that F-Secure may come into contact with Personal Data in the course of detecting or responding to a cyber threat. The processing is being conducted in order to guarantee security and to detect and respond to cyber threats. F-Secure collects data, largely, from three main sources 1.) Endpoints, 2.) Logs and 3.) Networks. Types of Personal Data are aggregated, which will include the processing of personal data such as:

- Usernames
- IP addresses
- E-Mail addresses (processes, execution artefacts, memory anomalies, network metadata (IP addresses, Hostnames)
- Network Adapters
- Registry
- Services
- Scheduled Tasks,
- Hooks / Threats
- Installed Programs and Features
- File Retrieval
- Map Filesystem and/or
- Appliance / Server logs

2. Purpose of data processing

Processing of the personal data takes places for the purposes of ensuring network and information security to prevent unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. The security insights will provide us with visibility of misuse or misconfiguration of existing security controls that – if left un-actioned – could increase the risk of successful attacks. F-Secure allows us to quantify a risk level specific environment and provides us with a prioritised set of recommendations on how the risk level can be reduced.

3. Legal basis for the processing of personal data

The legal basis for the processing of personal data is the user's given consent in accordance with Art. 6 (1) (1) (f) GDPR. For transfers of personal data to the UK, the UK has an EU Adequacy Decision according to Art. 45 GDPR. In addition, we signed standard contractual clauses according to Art. 46 (2) GDPR.

4. Duration of storage

Your personal information will be stored for as long as is necessary to fulfil the purposes described in this Privacy Policy or as required by law, e.g., for tax and accounting purposes.

5. Right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning yourself which is based on point (e) or (f) of Article 6 (1), including profiling based on those provisions.

Further information can be found at: https://www.f-secure.com/de/legal/privacy

This Privacy Policy has been created with the help of DataGuard.