



SFP Infrastructure Partners

Privacy Policy of the SFP Group

This Privacy Policy is displayed on the website of SFP Infrastructure Partners www.sfpinfra.com. SFP Infrastructure Partners is part of the Swiss Finance & Property Group.

1. Introduction/what is this Privacy Policy about?

Data protection and data privacy require trust and transparency. This is why we are explaining to you in this Privacy Policy how and for what purposes we collect, process and use your personal data.

Among other things, this Privacy Policy will tell you:

- what personal data we collect and process;
- for what purposes we use your personal data;
- who has access to your personal data;
- what benefits our processing of your data have for you;
- for how long we process your personal data;
- what your rights are with regard to your personal data; and
- how you can contact us.

We have aligned this Privacy Policy to the Swiss Data Protection Act as well as the European General Data Protection Regulation (GDPR). The GDPR has established itself globally as a benchmark for strong data protection. Whether and to what extent the GDPR is applicable depends on the individual situation.

We can make additional privacy policies available to you if this seems useful to us. Such additional privacy policies will supplement this Privacy Policy and have to be read together with this Policy.

2. Who are we?

We are Swiss Finance & Property Group AG ("SFP") and its subsidiaries ("SFP Group"), Seefeldstrasse 275, 8008 Zurich. As an independent fund management company and securities firm, we specialise in the entire value chain of real estate and infrastructure investments and combine our real estate and financial market expertise. We offer our products and services to investors in Switzerland while expanding into selected international markets.

The following companies are currently part of the SFP Group:

- Swiss Finance & Property Ltd, Zurich
- Swiss Finance & Property Funds Ltd, Zurich
- VIGA Re Management ApS, Copenhagen

- Swiss Finance & Property UK Ltd, London
- SFP Infrastructure Partners Ltd, Zurich
- Swiss Finance & Property Deutschland GmbH, Frankfurt
- SFP Investments Sàrl, Luxembourg
- SFP Investments GP Sàrl, Luxembourg
- SFP Retail AG
- SFP Commercial Properties AG

You can find more information about the SFP Group at www.sfp.ch.

3. Who is responsible for data processing?

Under data protection law, the party who is responsible for data processing is the person who determines whether the processing should be done, for which purposes it should be done, and how it is to be done. As the holding company of the SFP Group, Swiss Finance & Property Group AG, Seefeldstrasse 275, 8008 Zurich is responsible for the processing of data under this Privacy Policy.

If you have contact with a subsidiary of Swiss Finance & Property Group AG, this subsidiary too can be responsible for the relevant processing of data. In this case, any data protection provisions of the subsidiary in question will apply in addition to this Privacy Policy. For example, Swiss Finance & Property Ltd and, for tenants, Swiss Finance & Property Funds Ltd are also responsible for the processing of client data.

4. For whom and for what purposes does this Privacy Policy apply?

This Privacy Policy applies to all persons whose data we process (hereinafter referred to as "you"), regardless of the manner in which you establish contact with us, e.g. in person, on a website, by telephone, via a social network, at an event, etc. It applies to the processing of personal data previously collected by us as well as personal data to be collected in the future.

Our processing of data can apply to the following categories of persons in particular, provided that we process data in this case:

- Visitors to our website;
- Clients and business partners;
- Tenants;
- Service providers;
- Other persons who make use of our services or come into contact with our offers;
- Visitors to our offices;



SFP Infrastructure Partners

- Persons who write to us or establish contact with us in another manner;
- Recipients of information and market communications;
- Contact persons for our suppliers, buyers and other business partners as well as for organisations and government authorities.

Our contractual provisions can contain additional references to our data processing activities.

Please also consult these provisions. In addition, please read our policy on cookies for more information about the collection and processing of personal data in connection with the use of our websites and social media, in particular with regard to cookies and similar technologies.

5. What personal data do we process?

"Personal data" is information that can be linked to a specific person. We process different categories of personal data. The most important categories are explained below. In some cases, however, we can also process additional personal data.

You can find out more about the origin of this data in section 6 and the purposes for which we process this data in section 7.

5.1. Personal data of clients and business partners ("client data")

We capture the basic personal data of our clients and business partners and their employees, e.g. title, name, contact data, date of birth and information relating to their occupation and/or activities. We collect this data in particular in the context of existing or budding client and contractual relationships, based on personal contact (incl. business cards, email and telephone), when they complete a contact form, or subscribe to a newsletter or product updates. We also receive client data from third parties such as contact persons and representatives of contractual partners, organisations and government authorities.

We capture client data in our client relationship management system (CRM system). Once the data has been captured in our CRM system, a message is sent to the clients to inform them about this.

Client data includes, for example:

- Title, first name, surname, gender, date of birth;
- Address, email address, telephone number and other contact data;
- Information about your employer and your position/function in the company;
- Client accounting data (e.g. bank account details);
- Information about linked websites, social media profiles, etc.;
- Information about preferences and interests, language preferences, etc.;
- Information about your relationship with us;
- Information about related parties (e.g. contact persons, recipients of services or representatives);

- Settings regarding the delivery of marketing materials, subscribed newsletters, etc.;
- Information about your status with us (e.g. inactivity);
- Information about attendance of events;
- Official documents pertaining to you (e.g. identity documents, commercial register excerpts, licences, etc.); and
- Date and time of registrations.

5.2. Data of tenants ("tenant data")

SFP is the founder and/or manager of a number of collective investment vehicles (e.g. real estate funds or real estate companies) that hold properties in its portfolio. In cooperation with the relevant property manager we capture personal data of tenants in the context of the application process for rental properties and existing tenant relationships.

Tenant data includes, for example:

- Title, first name, surname, gender, date of birth, nationality;
- Address, email address, telephone number and other contact data;
- Information about their employment (employer, position/function, job description, income);
- Tenant accounting data (e.g. bank account details);
- Rental, dates of beginning and end of the tenant relationship;
- Information about the rented property, e.g. size, floor;
- Photos and copies of identification documents;
- Tenant consumption data (water, electricity, oil/gas, etc.);
- Amount of deposit and holder of deposit (bank or insurance company); and
- Other data, if any, e.g. relating to court or official procedures.

Please also take note of the separate privacy policy for the management company in question.

5.3. Data for the performance of contractual obligations ("contract data")

Contract data is personal data collected and processed by SFP in the interests of performing its contractual obligations. Contract data is personal data collected in the context of the conclusion and/or performance of the contract, e.g. information about the conclusion of the contract, contractual rights and obligations and contact data. We mainly enter into contracts with clients, business partners and service providers or, in the case of legal entities, with their contact persons.

Contract data includes, for example:

- Data relating to the initiation and conclusion of contracts, e.g. the date on which the contract is concluded, information about the application process and the relevant contract (e.g.



SFP Infrastructure Partners

type and duration or, if necessary, proof of identity such as copies of official identity documents);

- Information about the processing and management of contracts (e.g. contact information, delivery addresses, successful or unsuccessful deliveries and information about payment methods);
- Data pertaining to the client service and support in technical matters;
- Data pertaining to our interaction with you (at most a history with relevant entries);
- Information about defects and complaints as well as adjustments to contracts;
- Financial information (e.g. issue of invoices);
- Information about our interaction with you as the contact person or representative of a business partner; and
- Information about security checks and other investigations relating to the assumption or continuation of a business relationship.

5.4. Communication data

If you are in contact with us or we are in contact with you, e.g. when you contact a client relationship manager, we process the exchange of communication and information about the type, time and place of communication.

Communication data includes, for example:

- Name and contact information, e.g. postal address, email address and telephone number;
- Contents of emails, written correspondence, chat messages, social media messages, telephone conversations, video conferences, etc.;
- Information about the type, time and reason for the communication; and
- Metadata of the communication.

Telephone conversations and video conferences with us can be recorded, e.g. owing to regulatory requirements. We will inform you at the beginning of the conversation whether it will be recorded or not. If you do not wish us to record such conversations you can interrupt the conversation at any time and contact us via another medium (e.g. email).

5.5. Technical data

When you use our websites, wi-fi network or other electronic offers, we collect specific technical data, e.g. your IP address or device ID. Technical data also includes protocols recording the use of our systems (log files). Sometimes we can also allocate a unique identifying number (ID) to your end device (PC, smartphone, etc.) using cookies or similar technologies that allow us to recognise your device the next time you visit us.

We can in particular also use the technical data to obtain information about your behaviour, such as information about your website use. More information about this is provided in our cookie policy.

5.6. Film and sound recordings

When attending an event, for example, it can happen that we generate photos, videos or sound recordings in which you may also appear. For security and evidentiary purposes we also make videos of our offices and portfolio properties. These may provide us with information about your behaviour in these places. The use of video surveillance systems is limited to specific locations and is indicated.

Film and sound recordings include, for example:

- Recordings made by video surveillance systems;
- Photos, videos and sound recordings of client events and public events (e.g. trade fairs); and
- Recordings of telephone conversations and video conferences (owing to regulatory requirements).

6. Where does the personal data come from?

6.1. Personal data made available to us

You often make your personal data available to us yourself, for example when you subscribe to a newsletter, complete an application form as an interested tenant, enter into a contract with us, or communicate with us. In most cases you give us your client data, tenant data, contract data and communication data yourself.

You usually provide your personal data to us voluntarily, i.e. you are not obliged to give us your personal data. We must, however, collect and process some personal data in order to provide services and perform contractual obligations, in particular in the context of statutory provisions. Without such data we cannot provide services or perform contractual obligations.

When you send us data about third parties (e.g. work colleagues/employees), we assume that you are authorised to do so and that this data is correct. Please make sure that such persons have been informed about this Privacy Policy.

6.2. Collected data

We can also collect your personal data ourselves or as part of an automated process, e.g. when you call up our websites or click on a link in one of our newsletters. Most of the time this concerns technical data.

6.3. Received data

We can also receive personal data from other SFP Group companies. More information is provided in section 9.1. In addition, we can receive your personal data from other third parties, e.g. from business partners, persons who communicate with us, or public sources.

For example, we can receive your personal data from third parties in the following cases:

- From your employer, if you work for a company or a government authority;



SFP Infrastructure Partners

- From third parties, if correspondence and meetings refer to you;
- From persons from your environment (family, legal representatives, etc.), such as your contact details, references or powers of attorney;
- From the Swiss Post Office and from address dealers, e.g. for address updates;
- From banks, insurance companies, distribution and other contracting partners during sales and payment transactions;
- From providers of online services, e.g. providers of Internet analysis services;
- From providers of cyber security services;
- From information services in order to comply with statutory regulations such as those on the combating of money laundering;
- From government offices, parties and other third parties in connection with official and court proceedings;
- From media monitoring companies in connection with articles and reports that mention you;
- From public registers, e.g. debt collection office or commercial register, public institutions such as the Federal Statistical Office, from the media or the Internet.

7. For what purposes do we process the personal data?

7.1. Communication

As we wish to remain in contact with you and address your individual concerns, we process personal data in order to communicate with you, e.g. to answer queries and provide client support. To this end we in particular use client data and, where the communication concerns a contract, also contract data.

7.2. Conclusion and performance of contractual obligations, in particular management of tenant relationships

We process personal data in connection with budding, existing or terminated contractual relationships in the context of contract negotiations and contract executions, when preparing subscription documentation and subscription forms, and for the purpose of managing tenant relationships. This mainly involves contract data, tenant data and client data.

For example, the data is processed in order to:

- decide whether and how we wish to enter into a contract with you (including the credit check);
- provide the agreed benefits or agreed services;
- invoice our services and generally for accounting purposes;

- plan and prepare the delivery of our services, e.g. planning the deployment of our employees;
- check whether we want to and can work together with a company and to monitor and assess the services of this company;
- prepare and execute transactions under company law, e.g. purchases, sales and mergers of companies;
- enforce legal claims under contracts (debt collection, court proceedings, etc.);
- administer and manage our IT and other resources;
- store data in compliance with archiving requirements; and
- give notice of and terminate contracts.

7.3. Marketing and information

As we would like to send you news about SFP and our products and submit specific offers to you, if relevant, we process personal data for the purpose of cultivating relationships and for marketing purposes, e.g. to send you written and electronic messages and offers and to carry out promotions. This can pertain to our own offers or to offers by other companies for whom we work as distribution or placement agent.

Messages and information can be personalised to match your interests in order to only send you information that you are likely to find interesting. To this end we in particular use client, contract and communication data.

This can include the following messages and information, for example:

- Direct contact by employees of the client relationship management department;
- Newsletters, emails and other electronic messages;
- Advertising brochures, magazines and other printed matter; and
- Invitations to events.

For this we can use the contact data given to us by you. You can reject being contacted for marketing purposes at any time. With regard to newsletters and other electronic messages, you can unsubscribe the service via the link provided in the message.

7.4. Market evaluations and analyses

As we wish to constantly improve our services and react to market changes, we process personal data in order to prepare market evaluations and analyses. To this end we in particular process client and tenant data as well as technical data, and also analyse public surveys, studies and other information, e.g. data obtained from the media, the Internet and other public sources. We use pseudonymised or anonymised data for these purposes as far as possible.

We can carry out processing for the following purposes, for example, as part of market evaluations and analyses:



SFP Infrastructure Partners

- Execution of client surveys, reviews and studies;
- Optimisation and improvement of the user friendliness of websites;
- Statistical analyses;
- Market assessments with regard to the behaviour of our clients and tenants and the conduct of our competitors; and
- Market observation in order to understand current developments and trends and react to these.

7.5. Security

As we wish to provide the best possible security, we also process personal data for security purposes, in particular to guarantee IT security and for evidentiary purposes. This generally involves all data categories, but in particular also film and sound recordings and technical data. We can capture, analyse and store the data for the purposes mentioned.

To guarantee security we can carry out processing for the following purposes, for example:

- Preparing and analysing (manually and automatically) sound and video recordings in order to identify and prosecute punishable offences;
- Analysing system-related logs about the usage of our systems (log files);
- Preventing, warding off and investigating cyber attacks and malware attacks;
- Analysing and testing our networks and IT infrastructure as well as system and error checks;
- Controlling access to electronic systems (e.g. log-ins to user accounts);
- Physical access control (e.g. access to offices); and
- Documenting and preparing backups.

7.6. Compliance with legal provisions

As we wish to create the conditions required for compliance with legal provisions, we also process personal data in order to observe our legal obligations and to prevent and uncover breaches. This includes, for example, accepting and processing complaints and other notifications, complying with instructions from a court or a government authority, and implementing measures to uncover and investigate misuse and to store telecommunications metadata as prescribed by law (mobile phone subscription). This can apply to all categories of personal data.

In order to comply with the legal provisions we can carry out processing for the following purposes, for example:

- Investigating business partners;
- Accepting and processing complaints and other notifications;
- Storing telecommunications metadata as prescribed by law (mobile phone subscription);

- Carrying out internal investigations;
- Ensuring compliance and risk management;
- Disclosing information and documents to government authorities if we should have good cause to do so (e.g. because we are the injured party) or are obliged to do so by law (e.g. in the context of an internal or external audit);
- Cooperating with external investigations, e.g. by a prosecuting or supervisory authority;
- Ensuring the legally required data protection;
- Fulfilling information and notification obligations, e.g. in connection with supervisory and fiscal regulations such as archiving obligations and in order to prevent, uncover and investigate punishable acts and other breaches; and
- Combating money laundering and terrorism financing in compliance with the law.

All of these cases can be subject to Swiss or to foreign law as we are guided not only by self-regulatory, industry and other standards or official instructions, but also by our own corporate governance regulations.

7.7. Safeguarding of our rights

As we wish to be able to enforce our claims and defend ourselves against third-party claims, we also process personal data in order to safeguard our rights, e.g. to enforce claims before the court, prior to court proceedings or out of court, before Swiss and foreign authorities, or to defend ourselves against claims. Depending on the case we process different categories of personal data, in particular client and tenant data as well as contract data.

To safeguard our rights we can carry out processing for the following purposes, for example:

- Investigating and enforcing our claims, which can also include claims of our affiliated companies and our contracting and business partners;
- Defending against claims against us, our employees, our affiliated companies and our contracting and business partners;
- Analysing the chances of success in legal proceedings and other legal, business and other matters;
- Participating in proceedings before courts and authorities in Switzerland and abroad. For example, we can secure evidence, establish the chances of success of litigation or submit documents to an authority. The authorities may also require us to disclose documents and data carriers that contain personal data.

7.8. Administrative support within the SFP Group

As we wish to efficiently design our internal processes, we also process personal data for the internal administrative purposes of the SFP Group. To this end we in particular process client, tenant, contract, communication and technical data.

Administration can include processing for the following purposes, for example:



SFP Infrastructure Partners

- IT, risk and compliance management;
- Real estate management;
- Accounting;
- Archiving of data and management of our archives;
- Central storage and management of data that is used by several companies within the SFP Group;
- Review or execution of transactions under company law, e.g. purchases, sales and mergers of companies;
- Forwarding of enquiries to the responsible units; and
- General review and improvement of internal processes.

Like every group of companies, the SFP Group has an overall interest in ensuring the successful operations of its group companies, and our group companies are interested in their own activities and purposes of processing. We can therefore also disclose personal data to other companies of the SFP Group in order to support their own processing purposes under this Privacy Policy in the interests of the whole SFP Group.

8. On what lawful basis do we process personal data?

Depending on the purpose for processing, our processing of personal data is based on different lawful bases. We can in particular process personal data if processing:

- is required for the performance of a contract with you or the execution of pre-contractual measures (e.g. review of an application for a contract);
- serves to protect legitimate interests, e.g. where data processing is a central component of our business activities;
- is based on consent;
- is required for compliance with Swiss or foreign legal provisions.

We in particular have a legitimate interest in processing data for the purposes described in section 7 and the disclosure of data in accordance with section 9 and their related objectives. Legitimate interest refers to our own interests as well as the interests of third parties.

Legitimate interest includes, for example, interest in

- providing good client care, fostering relationships and communicating with clients, also outside of a contract;
- advertising and marketing activities;
- getting to know our clients and other persons better;
- improving our products and services and developing new ones;

- supporting the Group-internal management and communication processes that are essential for cooperation in a company that also employs part-time staff;
- providing mutual support for the activities and objectives of the Group companies;
- ensuring compliance and risk management as well as fraud prevention;
- protecting clients, other persons and the data, secrets and assets of the SFP Group;
- ensuring IT security, in particular in connection with the use of websites and other IT infrastructure;
- securing and organising business operations, in particular the operation and further development of websites and other systems;
- managing and developing the company;
- selling or buying companies, parts of companies and other assets;
- enforcing or defending against legal claims;
- complying with Swiss and foreign law as well as internal regulations.

9. To whom do we forward personal data?

9.1. Within the SFP Group

We can forward personal data received from you or from third-party sources to other companies of the SFP Group. Data can be forwarded in order to support the Group's internal administration or the relevant Group companies and their own processing purposes, such as when we assist in personalising marketing activities, developing and improving products and services or efforts to increase the general security. The relevant Group companies can also compare and link the personal data that is received to personal data that is already on hand.

This can include the following disclosures of data, for example:

- All the personal data categories mentioned in section 5, for managing and processing contractual relationships, in particular in connection with products and services that combine the input of several Group companies;
- Client data, tenant data, contract data and communication data, as well as findings from studies and public sources for market evaluations and analyses, where such data requires a personal reference;
- Client data, tenant data, contract data and communication data for the delivery and personalisation of offers, communication and marketing activities;
- Client data, tenant data, contract data and communication data for the prevention of fraud and money laundering;
- Client data, tenant data and data relating to film and sound recordings for evidentiary purposes;



SFP Infrastructure Partners

- Security-relevant data for security purposes and compliance with legal requirements;
- Data to support the safeguarding of rights.

9.2. Outside the SFP Group

We can also forward your personal data to companies outside the SFP Group when we make use of their services. As a rule, these service providers process personal data on our instructions as "order processors". Our order processors are obliged to process personal data exclusively in accordance with our instructions and to implement suitable measures to ensure data protection. Some service providers carry individual responsibility or share responsibility with us (e.g. real estate management companies), and in this regard we would ask you to take note of the privacy policies that may be sent to you by the service providers in question.

This can include services in the following areas, for example:

- Real estate management services;
- Financial services;
- Services pertaining to statutory audits or supervisory audits;
- Advertising and marketing services, e.g. for the delivery of notifications and information;
- Company management, e.g. accounting or asset management;
- IT services, e.g. data storage services (hosting), cloud services, delivery of email newsletters, etc.;
- Advisory services, e.g. services provided by tax consultants, lawyers, business consultants.

It can also happen that we forward personal data to other parties for their own purposes, e.g. if you have given us your consent or if we are obliged or authorised by law to forward the data. In such cases the recipient of the data is an independent controller under data protection law.

This includes the following cases, for example:

- Review or execution of transactions under company law, e.g. purchases, sales and mergers of companies;
- Disclosure of personal data to courts and authorities in Switzerland and abroad, e.g. to the prosecuting authorities if there is suspicion of punishable offences;
- Processing of personal data in order to comply with a court decree or official order or to enforce or defend against legal claims or when we consider it necessary for other legal causes. We can also disclose personal data to the other parties involved in legal proceedings.

Please also take note of our cookie policy for information about the independent collection of data by third-party providers whose tools are integrated into our websites and apps.

10. To whom do we disclose personal data abroad?

We mostly process and store personal data in Switzerland and the European Economic Area (EEA). In specific cases we can also disclose personal data to service providers and other recipients who are located outside of this area or who process data or have data processed by their own service providers outside of this area, i.e. in any country in the world. Such countries may not have laws that protect your personal data to the same extent as in Switzerland or the EEA. Where we transmit your personal data to such a country, we implement measures to ensure the adequate protection of your personal data.

Measures to ensure adequate data protection include, for example, the conclusion of data transfer contracts that apply the required data protection with the recipients of your personal data in third-party countries. These include contracts that have been approved, issued or recognised by the European Commission and the Federal Data Protection and Information Commissioner, known as standard contract clauses. Please note that while such contractual agreements partly compensate for weaker or lacking statutory protection, they cannot completely exclude all risks (e.g. state access abroad). In exceptional cases it may be permitted to transfer data to countries that do not apply adequate data protection, e.g. on the basis of consent, in connection with foreign legal proceedings, or if the transfer of data is required for the performance of a contract.

11. How do we protect your personal data?

We take suitable security measures of a technical and organisational nature to ensure the confidentiality of your personal data, to defend it against unauthorised or unlawful processing and to counteract the risks of loss, unintended amendment, involuntary disclosure or unauthorised access. Like all companies, we cannot entirely exclude breaches of data protection, and some residual risks unavoidably remain.

Technical security measures can include, for example, measures such as the encryption and pseudonymisation of data, protocols, access restrictions and the storing of backup copies. Organisational security measures can include, for example, directives to our employees, confidentiality agreements and controls. We also oblige our order processors to implement adequate technical and organisational security measures.

12. For how long do we process personal data?

We process and store your personal data for as long as

- required by the purpose of processing and/or the agreed purpose, for contracts usually at least for the duration of the contractual relationship;
- we have a legitimate interest in storing the data. This can in particular be the case if we need personal data to enforce or defend against claims, for archiving purposes and to guarantee IT security;



SFP Infrastructure Partners

- the data is subject to a statutory archiving obligation. Some data, for example, must be held in safe custody for a period of ten years. Shorter storage periods apply to other data, e.g. video surveillance recordings or records of specific Internet processes (log files).

We generally comply with the following archiving periods, but can deviate from these in individual cases:

- **Client and tenant data:** We store client and tenant data for at least ten years after the end of the client and/or tenant relationship. We can also store client and tenant data for longer for the purpose of cultivating relationships and for marketing purposes, and in anonymised form also for the purpose of market evaluations and analyses.
- **Contract data:** Contract data is usually stored for ten years after the last contractual activity or the end of the contract. The storage period can be longer if required for documentation purposes, for compliance with statutory or contractual provisions, or for technical reasons.
- **Communication data:** Emails, messages included in contact forms and written correspondence are usually stored for at least ten years or for ten years after the end of the relevant client or tenant relationship.
- **Technical data:** We usually store technical data for six months. The storage period for cookies mostly ranges from a few days to two years, unless they are deleted immediately after the end of the session.
- **Film and sound recordings:** The storage period depends on the purpose. It ranges from a few days for recordings by surveillance cameras to several years for reports about events that contain photos.

13. What are your rights in connection with the processing of your personal data?

You have the right to object to the processing of your data, in particular if we process your personal data on the basis of a legitimate interest and the other applicable conditions are met. You can also at any time object to the processing of your data in connection with direct marketing (e.g. advertising emails).

If the applicable conditions are met and no statutory exceptions apply, you also have the following rights:

- The right to ask us about your personal data stored by us;
- The right to have inaccurate or incomplete personal data rectified;
- The right to request the erasure or anonymisation of your personal data;
- The right to request restriction of processing of your personal data;
- The right to receive specific personal data in a structured, commonly used and machine-readable format;
- The right to revoke your consent with future effect where processing is based on consent.

Please note that these rights may in individual cases be limited or excluded, e.g. if there is doubt regarding your identity or this is required to protect other persons or overriding interests or to ensure compliance with statutory obligations.

You can contact us at any time if you wish to exercise one of the above rights or if you have questions about the processing of your personal data.

Please also contact us if you should doubt whether the processing of your personal data complies with the law. You can also file a complaint with the supervisory authority. The competent supervisory authority is the [Federal Data Protection and Information Commissioner \(FDPIC\)](#).

14. How can you contact us?

You are welcome to contact us at any time if you have any questions about this Privacy Policy or the processing of your personal data:

Swiss Finance & Property Group AG
Seefeldstrasse 275
8008 Zurich
Switzerland
Email: dataprotection@sfp.ch

You can also contact any of the other controllers.

15. Amendments to this Privacy Policy

We reserve the right to update and amend this Privacy Policy from time to time in order to take account of changes in the manner in which we process your personal data or to changes in the law. All future amendments to our Privacy Policy will be published on our website.