

PRIVACY POLICY OF CRIF AG FOR CREDIT RATING SERVICES

1. Introduction

Based on Article 13 of the Federal Constitution of the Swiss Confederation as well as the data protection provisions of the Swiss Confederation (Swiss Federal Act on Data Protection, FADP) and - where applicable - the EU General Data Protection Regulation (GDPR), every person has the right to protection of their privacy as well as protection against misuse of their personal data. The protection of your personal data is important to us. You can expect us to handle your data sensitively and carefully and to ensure a high level of data security.

This Privacy Policy explains how CRIF AG - hereinafter also referred to as “we” - collects and further processes personal data, insofar as this is not apparent from the circumstances or regulated by law.

2. Identity and contact details of the controller

The data controller within the meaning of the Swiss Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR) is:

CRIF AG
Hagenholzstrasse 81
8050 Zurich, Switzerland
VAT ID: CHE-107.708.282

Email: info.ch@crif.com
Website: www.crif.ch

CRIF AG has not appointed a data protection advisor or data protection officer within the meaning of Art. 10 FADP or Art. 37 GDPR. Any enquiries, claims or information relating to data protection law should be sent to the aforementioned contact details of the controller.

3. Purpose of the processing and legal basis

We process your personal data mentioned under section 4 below for the following purposes:

- *To provide information for the purpose of establishing the identity and checking the creditworthiness of the data subject, preventing abuse, fulfilling customer verification obligations (in particular in connection with combating money laundering and the funding of terrorism and corruption, and the protection of participants in games of chance and the*

verification of consumer loans) and for the purpose of comparison with sanctions lists (Art. 30 and Art. 31 (1) and (2) lit. c FADP / Art. 6 (1) lit. f GDPR): This purpose includes the services of a credit agency with management of credit risks (calculation of a future probability of default).

- *For the conclusion and processing of your contractual relationship and for processing your enquiries or your orders (Art. 30 and Art. 31 (1) and (2) lit. a FADP / Art. 6 (1) lit. b GDPR):* The purposes of the data processing depend on the intended transaction. We collect these data in order to provide you with our services or to be able to obtain such services from you.
- *For the management of our website (Art. 30 and Art. 31 (1) and (2) lit. b FADP / Art. 6 (1) lit. b and f GDPR):* This includes, in particular, the administration of the users of the website and the activities carried out thereon, the management and further development of the website, the provision of a flawless connection, the evaluation of system security and stability and other administrative purposes.
- *For process and offer optimisation (Art. 30 and Art. 31 (1) and (2) lit. e FADP / Art. 6 (1) lit. a and f GDPR):* This includes quality control, the preparation of statistics, budget and management information as well as their evaluation, market research, the further development of products and services and of the company and its processes.
- *For marketing and advertising purposes (Art. 30 and Art. 31 (1) FADP / Art. 6 (1) lit. a and f GDPR):* This includes customer loyalty, the implementation of customer loyalty programmes, the optimisation of customer offers, market or opinion research and the organisation of customer events. You may object at any time to any processing or use of your data for direct marketing purposes. The objection must be addressed to the controller.
- *For compliance with legal and regulatory requirements (Art. 30 and Art. 31 (1) FADP / Art. 6 (1) lit. c GDPR):* We process your data to comply with the statutory obligations imposed on us. This includes the processing of data within the scope of obligations to provide information to authorities as well as compliance with tax and/or commercial law regulations (e.g., obligations to retain business and accounting documents).
- *For the sale or purchase of business divisions, companies or parts of companies and other transactions under company law (Art. 30 and Art. 31 (1) FADP / Art. 6 (1) lit. a and f GDPR).*

4. Categories of personal data processed

The following categories of personal data may be processed by us in connection with our services:

- *Identity data:* This includes in particular, but is not limited to, first and last name(s), birth name(s), dates of birth and death, place or country of birth or residence, gender, title, academic degree, citizenship, marital status, spouse, occupations, links to legal

entities including roles, address, registered office, telephone number, fax, email, website URL.

- *Data for business transactions with our customers and prospective customers:* This includes in particular, but is not limited to, information on previous business transactions, data retrieved by customers from the CRIF database (“query data”, including any order data contained therein), information on business enquiries, offers, conditions and contracts on products and services supplied and sold as well as ordered and purchased, information in connection with queries, complaints and disputes on products and services or the contracts concluded in relation thereto, such as warranty and guarantee cases, rescissions, etc.
- *Data on recruitment:* This includes in particular, but is not limited to, information for our human resource planning and management or to ensure appropriate staffing, data for investment decisions, as well as for planning and managing the skills of potential employees and for planning to process applications received through various channels (e.g., via email or LinkedIn) and to be able to refer to applications received for potential employment at a later stage.
- *Data for internal human resources:* This includes in particular, but is not limited to, information about our employees such as the “OASI” number, religious denomination, date of marriage, name of spouse, name and date of birth of children, bank/postal details, date of entry/exit, title, role, career, education, salary data incl. social contributions, criminal record certificate, family allowance statement, data on accident or illness, working hours and appraisals.
- *Payment experience data in connection with our activities as a credit reference agency:* This includes data on compliance with payment terms and on undisputed claims that have not been paid after the due date and for which multiple reminders have been sent, as well as data on enforcement measures and data from debt collection reports.
- *Data for assessing creditworthiness in connection with our activities as a credit agency:* Such as aggregated creditworthiness criteria and score values.

The consumer credit score is a statistical measure that predicts the probability of a payment incident over the following 12 months. Scores in the red range indicate a high probability of default. Scores in the yellow range indicate a medium probability of default. Scores in the green range indicate a low probability of default. The higher the number of points, the less likely a default. The score of individuals with negative payment experiences (such as loss certificates, debt repayment orders, debt collection cases) is essentially determined by the following three factors: number, status and timeliness of known payment experiences. The greater the number of individual events, the more serious the status of each individual event and the more recent the individual events are, the higher they are weighted. For individuals with exclusively positive payment experiences (paid bills) or for whom no payment experiences are known at all, the score is in the green range. In this case, the score is calculated mainly on the basis of official registries and public publications (commercial register, debt collection statements, cantonal official gazettes, telephone book), socio-demographic factors (such as age,

profession, nationality) and positive payment experiences. Being older, being known to the credit agency for longer and more positive information result in an even higher score. The business credit score is a statistical measure that predicts the probability of a serious payment incident over the following 24 months. Scores in the red range indicate a high probability of default. Scores in the yellow range indicate a medium probability of default. Scores in the green range indicate a low probability of default. The higher the number of points, the less likely a default. The score is essentially determined by the following three factors: number, status and timeliness of known payment incidents. The greater the number of individual events, the more serious the status of each individual event and the more recent the individual events are, the higher they are weighted.

- *Company-related data:* This can be information on the size of the company and the number of employees or data from the commercial register such as VAT ID number, functions of corporate bodies including powers of attorney and purpose of the company, as well as commercial data (data on trade licence, description of activities or sector) and information from media observations and researched data (e.g., on ownership).
- *Financial data,* such as bank account details, payment details, credit card details and other payment details, billing and shipping addresses, payment details for making online payments, etc.
- *Data related to the marketing of products and services:* This includes in particular, but is not limited to, information about marketing activities such as receipt of newsletters, newsletter opt-ins and opt-outs, documents received, invitations and participation in events and special activities, personal preferences and interests, etc.
- *Data in connection with the use of the website:* This includes in particular, but is not limited to, IP address and other identifiers (e.g., user name for social media, MAC address of smartphones or computers, cookies, web beacons, pixel tags, log files, local shared objects (Flash cookies) or other technologies that automatically collect personal data), date and time of the visit or use of the websites, pages and content accessed, referring websites, etc. (cf. also section 8 below).
- *Data concerning sustainability:* Information on social, environmental, societal aspects, such as energy consumption, certifications, management with corresponding scores.
- *Third-party data:* If you provide us with personal data of third parties (e.g., subcontractors, employees, etc.) in the course of a business transaction, we also process these data.
- *Data and documents relating to personal documentation (e.g., ID, passport, driving licence) and pictures for identification in the case of requests for information.*
- *Land registry data and building data (data on the building assigned to an address).*
- *Data from public registries and notices pursuant to Art. 35 SchKG [Swiss Debt Enforcement and Bankruptcy Law]:* For example, data from the residents' registration

office, notifications of the opening of bankruptcy proceedings, probate or creditors' meetings.

- *Blocking notes according to Robinson list*
- *Indications of abusive or potentially abusive behaviour: E.g., in the case of attempts to deceive identity, address or creditworthiness in connection with contracts for telecommunications services or contracts with credit institutions or financial service providers or in (internet) commerce.*
- *Assessment with regard to deliverability for addresses*
- *Source of the data and classification of the source as well as details on the corresponding data collection*
- *Indicators of a risk of abuse, such as information on the existence of a person or information on the prevention of fraud*

We do not process any particularly sensitive personal data within the meaning of Art. 5 lit. c FADP, do not carry out any high-risk profiling (Art. 5 lit. g FADP) and do not make any automated individual decisions within the meaning of Art. 21 (1) FADP. CRIF AG itself does not make any decisions, but merely supports its contracting partners with its information in the decision-making process. The risk assessment and evaluation of creditworthiness is carried out solely by the business partner, as this entity alone has the additional information required for this.

5. Categories of recipients of data

In principle, without your express prior consent, your personal data will be transferred only to the recipients named below:

- *Clients/partners of CRIF AG with a legitimate interest in the information provided in each case:* These are, in particular, companies in the credit industry and (internet) commerce that make advance payments to data subjects (e.g., purchase on open account, granting credit, credit card business, etc.), companies that are subject to statutory inspection obligations and lessors. Only business partners of CRIF AG who have entered into a written contractual relationship in which they undertake to comply with all applicable provisions of data protection law may obtain data.
- *Companies that belong to our Group:* A list of the Group companies is available at the following link: <https://www.crif.com/about-us/our-global-presence/>; these companies include our parent company, CRIF S.p.A, whose Privacy Policy is available at <https://crifsg.com/global/#InfoPrivacy> and <https://www.crif.it/informativa-sul-trattamento-dei-dati-personali-per-finalità-di-informazione-commerciale/>.
- *Public bodies and authorities:* If it is necessary to clarify an illegal use of our services or for legal prosecution, personal data will be forwarded to the law enforcement authorities and, if necessary, to injured third parties. However, this will happen only if

there are concrete indications of unlawful or abusive behaviour. Disclosure may also take place if it serves to enforce terms of use or other agreements. We are also required by law to provide information to certain public bodies upon request. These are law enforcement authorities, authorities that prosecute administrative offences subject to fines and the tax authorities. The disclosure of these data is based on our legitimate interest in combating abuse, prosecuting criminal offences and securing, asserting and enforcing claims, Art. 30 and Art. 31 (1) FADP and Art. 6 (1) lit. f GDPR.

- *Contract processors:* We may use contracted external service providers (“contract processors”) to provide our services. In such cases, personal data will be transferred to these contract processors to enable them to continue processing. These contract processors are carefully selected and regularly audited by us. The contract processors may use the data only for the purposes specified by us and are also contractually obliged by us to handle your data exclusively in accordance with this Privacy Policy and the applicable data protection laws.

For example, we use IT service providers to provide cloud services, software and hardware and to carry out maintenance work.

The transfer of data to contract processors is based on Art. 9 FADP or Art. 28 (1) GDPR, alternatively on our legitimate interest in the economic and technical benefits associated with the use of specialised contract processors and the fact that your rights and interests in the protection of your personal data do not prevail, Art. 31 (1) FADP or Art. 6 (1) lit. f GDPR.

6. Data transmission outside of Switzerland

Your personal data will always be processed in Switzerland. However, we may transfer your data to trusted recipients in third countries (both in the European Union and elsewhere in the world).

This transfer will take place on the basis of what is known as an adequacy decision of the Swiss Federal Council or the European Commission. If a recipient is located in a country without adequate statutory data protection, we oblige the recipient to comply with the applicable data protection on the basis of suitable guarantees pursuant to Art. 16 (2) FADP or Art. 46 (2) GDPR, in particular by means of what are called standard contractual clauses, which have also been issued by the European Commission or recognised, issued or approved by the Swiss Federal Data Protection and Information Commissioner (FDPIC). We can dispense with such an obligation if we can rely on an exemption clause. An exception may apply in particular in the case of legal proceedings abroad, but also in cases of overriding public interests or if the processing of a contract requires disclosure abroad, if you have consented or if the data in question were made generally accessible by you and you have not objected to their processing.

We transfer the data provided to companies belonging to our Group - a list of Group companies is available at the following link:

<https://www.crif.com/about-us/our-global-presence/>; these companies include our

parent company, CRIF S.p.A, Italy, whose Privacy Policy is available at: <https://crifsg.com/it/#InfoPrivacy> and <https://www.crif.it/informativa-sul-trattamento-dei-dati-personali-per-finalità-di-informazione-commerciale/>. In the present case, it cannot be ruled out that data will be transmitted outside the European data protection area, in particular also to recipients in the USA. Please also note that data exchanged via the internet is often routed via third countries. Your data may therefore pass through other countries even if the sender and recipient are in the same country.

7. Duration of storage

The deletion period regulates the time from when personal data must be deleted. The following deletion periods apply regardless of whether the underlying data were collected and stored on a statutory basis or on the basis of consent. The data must be deleted by the end of this period at the latest.

We store your personal data for as long as (i) statutory retention obligations exist or (ii) any legal claims for the assertion or defence of which the personal data are required have not yet become time-barred.

Otherwise, your personal data will be kept by us at most until the purpose on which the processing is based (see section 3 above) has ceased to apply. For archiving purposes, the data can also be stored for longer.

The statutory deletion period for creditworthiness data is 10 years. Receivables and payment experiences that have not been pursued will be deleted by us after only 5 years.

8. Automated data collection and processing on our website

We use various technologies on our website that enable us and third parties we engage to recognise you when you use our website and, in some circumstances, to track you across multiple visits. We will inform you about these in this section.

Essentially, this is so that we can distinguish your access (via your system) from access by other users, so that we can ensure the functionality of the website and carry out evaluations and customisations. We do not intend to infer your identity in doing so, although we may be able to do so insofar as we or third parties engaged by us can identify you by combining the data with registration data. Even without registration data, however, the technologies used are designed in such a way that you are recognised as an individual visitor each time you access the site, for example by our server (or the servers of third parties) assigning you or your browser a specific identification number (i.e., a “cookie”).

We use such technologies on our website and allow certain third parties to do so as well. However, depending on the purpose of these technologies, we may ask for your consent before they are used. You can adjust your current cookie settings on the website at any time. You can program your browser to block or deceive certain cookies or alternative

technologies, or to delete existing cookies. You can also use a browser extension that blocks tracking by certain third parties. You can find further information on this on the help pages of your browser (usually under the keyword “data protection”) or on the websites of the third parties.

A distinction is made between the following cookies (technologies with comparable functions such as fingerprinting are included here):

- *Essential cookies:* Some cookies are necessary for the functioning of the website as such or for certain features. For example, they ensure that you can switch between pages without losing information entered in a form. They also make sure you stay logged in. These cookies only exist temporarily (“session cookies”). If you block them, the website may not work. Other cookies are necessary so that the server can save decisions or entries made by you beyond one session (i.e., one visit to the website) if you request this function (e.g., language selected, consent given, the function for automatic login, etc.).
- *Performance cookies:* In order to optimise our website and corresponding offers and to better adapt them to the needs of users, we use cookies to record and analyse the use of our website, possibly also beyond the session. We do this through the use of third-party analytics services. We have listed these below. Before we use such cookies, we ask for your consent. You can revoke this at any time via the cookie settings.

We currently use offers from the following service providers and advertising contract partners (insofar as they use data from you or cookies set on your computer for advertising purposes):

- *Google Analytics:* Google Ireland (based in Ireland) is the provider of the “Google Analytics” service and acts as our contract processor. Google Ireland also relies on Google LLC (based in the USA) as its contract processor (hereinafter referred to together as “Google”) for this purpose. Google uses performance cookies (see above) to track the behaviour of visitors to our website (duration, frequency of pages viewed, geographical origin of access, etc.) and compiles reports for us on the use of our website on this basis. We have configured the service so that the IP addresses of visitors are truncated by Google in Europe before being forwarded to the USA and thus cannot be traced. We have switched off the “Data sharing” settings and switched on “Signals”. Although we can assume that the information we share with Google does not constitute personal data for Google, it is possible that Google can draw conclusions about the identity of visitors from these data for its own purposes, create personal profiles and it is also certain that Google links these data to the Google accounts of people who have consented to personalised advertising. If you consent to the use of Google Analytics, you explicitly agree to such processing, which also includes the transfer of personal data (in particular website and app usage data, device information and individual IDs) to the USA and other countries. Information on the data protection of Google Analytics is available here [<https://support.google.com/analytics/answer/6004245>], and if you have a Google account, you can find further details on processing by Google here [<https://policies.google.com/technologies/partner-sites?hl=en>].

- **Google Ads:** Our website uses Google Conversion Tracking. If you have accessed our website via an ad placed by Google, Google Ads will set a “cookie” (see above) on your computer. These cookies lose their validity after 30 days and are not used for personal identification. If the user visits certain pages of our website and the cookie has not yet expired, we and Google can recognise that the user has clicked on the ad and been redirected to this page. Each Google Ads client receives a different cookie. Cookies can therefore not be tracked across Ads clients’ websites. The information collected using the conversion cookie is used to create conversion statistics for Ads clients who have opted in to conversion tracking. Clients learn the total number of users who clicked on their ad and were redirected to a page tagged with a conversion tracking tag. However, they do not receive information that can be used to identify users personally. If you do not wish to participate in the tracking, you can refuse the setting of a cookie required for this - for example, by means of a browser setting that generally deactivates the automatic setting of cookies, or by setting your browser in such a way that cookies from the domain “googleleadservices.com” are blocked. Please note that you must not delete the opt-out cookies as long as you do not want any measurement data to be recorded. If you have deleted all your cookies in the browser, you must set the respective opt-out cookie again. The legal basis for the processing of personal data using Google Ads is Art. 30 and Art. 31 (1) FADP and Art. 6 (1) lit. f GDPR.

9. Your rights in connection with the processing of your personal data

Right to information (Art. 25 FADP or Art. 15 GDPR): You have the right to request information about your personal data processed by us at reasonable intervals. Upon request, we will provide you with a copy of the data that are the subject of the processing.

Right to rectification (Art. 32 FADP or Art. 16 GDPR): You have the right to request that we correct incorrectly processed data.

Right to withdraw consent (Art. 6 (6) and Art. 31 (1) FADP or Art. 7 (3) GDPR): If the data processing by us is based on your consent, you have the right to revoke any consent given to us at any time. The lawfulness of the processing carried out on the basis of the consent up to the revocation remains unaffected by the revocation.

Right to restriction of processing (Art. 30 (2) lit. b FADP or Art. 18 GDPR): Under certain conditions, you have the right to restrict the processing of your personal data (e.g., with regard to the duration of use, the material reference or the purpose of the processing, etc.). In such a case, we may continue to process the data in the previous manner only if there is a legally provided justification.

Right to erasure (Art. 30 (3) FADP or Art. 17 GDPR): You furthermore have the right to request that we delete your personal data. Among other things, we are obliged to delete your personal data if you expressly prohibit us from processing them and there is no justifiable reason for further processing, if your personal data are no longer required for

the purposes for which they were collected or otherwise processed, if you have withdrawn previously granted consent or if the data have been processed unlawfully.

It is not possible to delete or block individual payment experiences. However, you have the option to correct such information if there are errors. In the case of publicly published data relevant to creditworthiness, blocking or deletion is not possible.

If you request deletion, CRIF AG will block all your data for any queries. However, the identification data are not deleted; this is to ensure that a data subject is not re-entered into the database with a new registration.

Right to data portability (Art. 28 FADP or Art. 20 GDPR): Where we process your data automatically for the conclusion or performance of a contract or with your consent, we shall, at your request, release these data to you in a machine-readable format or - at your option - transfer it to a third party.

Right to object (Art. 21 GDPR): If we process your data for the performance of a task in the public interest or in the exercise of official authority (Article 6 (1) clause 1 lit. e GDPR) or if the data processing is based on our legitimate interests, you have the right, on the basis of the GDPR, to object to the processing of your personal data at any time for reasons arising from your particular situation. We will then stop the processing unless we can demonstrate compelling legitimate grounds for the processing that override your interests in stopping the processing.

You can object to the processing of your personal data for direct marketing purposes at any time without restrictions.

Right to lodge a complaint (Art. 49 FADP or Art. 77 GDPR): Insofar as applicable to you, there is a right to lodge a complaint with a competent data protection authority. The supervisory authority which is competent in Switzerland can be contacted at the following address: Federal Data Protection and Information Commissioner, Feldeggweg 1, CH 3003 Bern, Switzerland.