Privacy Policy

As of: 30.08.2026

1. General

1.1 Subject matter and scope

1.1.1 The protection of personal data is an important concern for us. This Privacy Policy informs about which personal data SF2 Systems GmbH processes when visiting its website https://sf2systems.com as well as when using the associated user account, order, download, license, support, and communication functions, for what purposes the processing takes place, on which legal bases it is based, and which rights data subjects have.

1.1.2 Personal data are all information relating to an identified or identifiable natural person.

1.2 External websites

1.2.1 Our website may contain links to third-party websites. The operator of those websites is generally responsible for the processing of personal data that occurs there. The privacy policy of the respective provider applies.

2. Responsible Party

2.1 Responsible Entity

2.1.1 The responsible party within the meaning of the General Data Protection Regulation is:

SF2 Systems GmbH
Eichelhofstraße 2B
1190 Vienna
Austria

E-mail: info@sf2systems.com

2.2 Contact for Data Protection Matters

2.2.1 Questions regarding the processing of personal data as well as requests to exercise data protection rights can be directed to the email address mentioned above.

3. Accessing the Website and Server Log Data

3.1 Processing when accessing the website

3.1.1 When accessing our website and the associated online services, technically required connection and access data are processed. These include, depending on the access, in particular: a) IP address; b) date and time of access; c) accessed page or file; d) browser type and browser version; e) operating system used; f) referrer URL, if transmitted by the browser; g) access status; h) amount of data transmitted; and i) other technically necessary connection and error data.

3.1.2 The processing serves the technical provision of our website and online services, ensuring stability and functionality, error analysis, as well as the detection and prevention of unauthorized access, misuse, and other security incidents.

3.2 Legal Basis and Retention Period

3.2.1 The legal basis is Art. 6 para. 1 lit. f GDPR. Our legitimate interest lies in the secure, stable, and trouble-free operation of our website and IT systems as well as in the prevention of abusive or unauthorized access.

3.2.2 Server log data is generally deleted after 30 days. Any storage beyond this period only occurs to the extent necessary for the investigation of a specific security or abuse incident, to comply with legal obligations, or to assert, exercise, or defend legal claims.

4. Contact and General Inquiries

4.1 Processing of Contact Data

4.1.1 If you contact us by e-mail, via a contact form, or by other electronic means, we process the data you provide in the context of contacting us. This may include in particular: a) Name; b) Company; c) E-mail address; d) Telephone number, if provided; e) Content of your message; f) Attachments you send; and g) Time and course of communication.

4.1.2 Processing is carried out to handle your request and for further communication with you. If the request is aimed at initiating or executing a contract, the processing is based on Art. 6 para. 1 lit. b GDPR. Otherwise, it is carried out on the basis of Art. 6 para. 1 lit. f GDPR; our legitimate interest lies in the proper handling and traceable documentation of incoming requests.

4.2 Storage duration

4.2.1 The data will be deleted as soon as the request has been finally processed and no legal retention obligations, ongoing contractual relationships, or other legitimate reasons for further storage oppose this.

5. SF2 User Account

5.1 Creation and management of a user account

5.1.1 For the setup and management of an SF2 user account, we process the master data and technical information required for this purpose. This includes in particular: a) full name; b) email address; c) company, if provided; d) authentication data, in particular an encrypted password hash; e) user or user account identifier; f) registration and confirmation status; g) date and time of registration and email confirmation; h) login and security-related event data; and i) temporary identifiers for email confirmation and password reset.

5.1.2 The processing serves the provision and management of the user account, the authentication of the user, access to software downloads, download history, license functions, orders, and personal settings, as well as the protection of the user account against unauthorized access.

5.2 Contract, consent, and evidence data

5.2.1 To the extent necessary for the execution or documentation of legally relevant processes, we additionally process in particular: a) the time and status of contract conclusions and license activations; b) the version of the Terms and Conditions; c) the version of the license terms included at the respective time; d) the version of these provided at the respective time Privacy Policy; e) timing, content, and status of voluntary consents; f) changes and withdrawals of such consents; g) if necessary, evidence of declarations related to immediate contract performance and the expiration of a statutory right of withdrawal; h) changes to user account or contract data, as well as i) renewal, modification, termination, and other legally relevant status information.

5.2.2 These data serve in particular for contract processing, traceability of legally significant declarations, as well as compliance with statutory accountability and documentation obligations.

5.3 Legal bases

5.3.1 The processing for the setup and management of the user account as well as for carrying out associated contractual and license relationships is based on Art. 6(1)(b) GDPR. Security-relevant processing is additionally based on Art. 6(1)(f) GDPR; our legitimate interest lies in securing user accounts as well as in detecting and preventing unauthorized or abusive access.

5.3.2 As far as data is processed to fulfill statutory accountability, documentation, or proof obligations, the processing is carried out on the basis of Art. 6 para. 1 lit. c GDPR. To the extent that documentation beyond this is necessary to assert, exercise, or defend legal claims, processing may be based on Art. 6 para. 1 lit. f GDPR.

5.4 Storage Duration

5.4.1 User account data is generally stored as long as the respective SF2 user account exists. After the deletion of a user account, personal data is removed, provided there are no statutory retention obligations, ongoing contractual or license relationships, or other legitimate reasons for further storage.

5.4.2 The deletion of an SF2 user account therefore does not necessarily lead to the simultaneous deletion of all contract, invoice, license, or verification data.

5.4.3 Confirmation and temporarily valid identifiers for resetting the password are deleted or technically invalidated after their use or after their validity expires.

6. Software downloads and download history

6.1 Processing in the download area

6.1.1 In a software download, the following data in particular may be processed: a) user account or user identifier; b) selected product; c) software version; d) platform or system architecture; e) date and time of the download; f) download status; g) IP address and technical access data; and h) number or history of downloads.

6.1.2 The processing serves the provision of the requested download, the display of the personal download history, the traceable assignment of software versions, as well as the protection of the download infrastructure against misuse and automated or unauthorized access. It may also be necessary in order to assign requests for technical support for a specific software version.

6.2 Legal Basis

6.2.1 The processing is carried out on the basis of Art. 6 para. 1 lit. b GDPR. Insofar as it serves security or misuse prevention, it is additionally based on Art. 6 para. 1 lit. f GDPR.

6.2.2 Any further analysis of visiting or usage behavior on our website is carried out exclusively in accordance with Section 12 of this Privacy Policy.

7. License Activation and License Management

7.1 Processed License Data

7.1.1 For the creation, activation, provision, and management of an SF2 license, we process, depending on the license model, in particular: a) full name; b) company; c) email address; d) product and license type; e) license ID; f) hardware ID of the licensed target system; g) public key of the target system (Device Public Key), if provided; h) issuance date; i) validity period for time-limited licenses; j) activation and confirmation status; k) licensed features or instances; l) renewal, modification, or termination status; and m) technical signature and license metadata.

7.1.2 The processing is necessary to check the license entitlement, to create and provide a signed and, if applicable, device-bound license file, to manage existing license rights and durations, as well as to document extensions, changes, and terminations in a traceable manner. It also enables the assignment of issued licenses in response to technical support, security, or license management inquiries.

7.2 Legal basis and storage duration

7.2.1 The processing is carried out on the basis of Art. 6 para. 1 lit. b GDPR. To the extent that it serves to prevent license abuse, to secure the activation process, or to ensure the traceability of issued licenses, it is additionally based on Art. 6 para. 1 lit. f GDPR.

7.2.2 The core data required for a license is generally stored for the duration of the existing license entitlement. For licenses without a time limit, this may mean storage for the duration of the ongoing license entitlement.

7.2.3 After the termination of a license, data is only further stored to the extent required due to legal obligations, for purposes of technical support, for abuse prevention, for documentation of existing or previous license rights, or for asserting, exercising, or defending legal claims.

7.2.4 Information that is explicitly marked as optional in the respective activation process does not have to be provided.

7.3 Local license verification after provisioning

7.3.1 After the license code or the license file has been provided, the technical checks of the license entitlement are carried out locally on the respective system. No periodic online queries to SF2 Systems are conducted for these ongoing checks.

7.3.2 In particular, no license ID, hardware ID, target system, instance, or other license check data is periodically transmitted to SF2 Systems for the local license check after the provision. Data that the user sends to SF2 Systems themselves in the context of a new activation, modification, support, or other expressly requested process remain unaffected.

8. Orders, contract processing, payment processing, and invoicing

8.1 Order and billing data

8.1.1 For paid orders through our shop, we process the data that is required for contract conclusion, contract processing, payment allocation, and invoicing. Depending on the transaction, this particularly includes: a) name; b) company; c) billing address; d) email address; e) VAT number, if provided or required; f) ordered products, licenses, or services; g) order and contract data; h) invoice amount and currency; i) chosen payment method; j) payment status; k) payment and transaction references; l) invoice data; and m) information on refunds, cancellations, or other payment-related transactions.

8.2 Payment processing via Mollie

8.2.1 For the processing of electronic payments, we use Mollie B.V., Netherlands, as a payment service provider. To carry out the payment, the customer is redirected to the payment environment provided by Mollie. The payment data required for the chosen payment method is collected directly by Mollie there.

8.2.2 Full credit or debit card numbers, card verification numbers such as CVC, or online banking access data are not transferred to SF2 Systems and are not stored by SF2 Systems.

8.2.3 SF2 systems store the invoice, order, and transaction data required for processing and documenting the order. This specifically includes the payment ID assigned by Mollie, payment status, payment method, as well as the internal references necessary to assign the payment transaction.

8.2.4 Depending on the chosen payment method and the information provided by Mollie in the respective payment transaction, additional payment metadata may also be processed. This may particularly include masked card information or information about a bank account used for the payment. Such information is only processed to the extent necessary for the execution or documentation of the order, the allocation of the payment receipt, invoicing, refunds, the handling of payment issues, or for corresponding proof purposes.

8.2.5 Mollie processes the personal data required for the respective payment within the framework of payment processing under its own data protection responsibility. This particularly includes the execution of the payment as well as, where applicable, the fulfillment of its own legal obligations and measures for fraud and abuse prevention. The data protection provisions of Mollie also apply to this processing.

8.3 Legal bases and retention period

8.3.1 The processing for the execution of the order and the associated contract is based on Art. 6 para. 1 lit. b GDPR. To the extent that data is processed to fulfill legal invoicing, accounting, tax, or retention obligations, the processing is based on Art. 6 para. 1 lit. c GDPR.

8.3.2 Contract and order data are stored for the duration of the respective contractual relationship and beyond for as long as this is required due to statutory retention or limitation periods. Invoices, booking vouchers, and other documents required to be retained for tax or corporate law purposes are generally kept for the legally prescribed period, usually seven years. Longer statutory retention periods remain unaffected.

9. Technical Support and Error Analysis

9.1 Processing in Support and Error Cases

9.1.1 If you request technical support or report an error to us, we process the data necessary to handle the respective case. This may in particular include: a) name; b) company; c) email address; d) product and version information; e) license ID; f) if applicable, hardware ID; g) content of the request; h) technical error messages; i) diagnostic or log data; j) voluntarily submitted files; and k) history of communication as part of the technical support.

9.1.2 The processing serves the handling of the request for technical support, the analysis and correction of errors, the examination of technical or license-related issues, as well as communication with the user. Insights from technical support processes can also be used to improve the stability and security of our products and services.

9.2 Legal basis and storage duration

9.2.1 Insofar as technical support is part of an existing contractual or license relationship, the processing is carried out on the basis of Art. 6 para. 1 lit. b GDPR. Otherwise, it may be based on Art. 6 para. 1 lit. f GDPR; our legitimate interest lies in properly supporting our users as well as correcting and preventing technical errors.

9.2.2 Data from technical support processes are stored for as long as this is necessary for processing the respective process and for appropriate technical traceability. Longer storage occurs only to the extent required by legal or contractual obligations or if the data are needed to assert, exercise, or defend legal claims.

10. Sensor, machine, and operational data

10.1 Local processing by SF2 software

10.1.1 The use of SF2 software does not by itself lead to an automatic transmission of the sensor, machine, or operational data processed with the software to SF2 Systems. As long as the software is operated locally or within the user's infrastructure, the data processed there generally remain within the respective user or customer environment.

10.2 Separate transmission to SF2 Systems

10.2.1 Processing of such data by SF2 Systems only takes place if data is transmitted to or made accessible to SF2 Systems as part of a separate service or communication. This can occur, for example, in the context of technical support, error analysis, a feasibility or evaluation check, a project, an analysis or consulting service, or any other separately agreed service.

10.2.2 If such data contains personal information, the data protection role of SF2 Systems depends on the respective service and the specific circumstances. Insofar as SF2 Systems processes personal data exclusively on behalf of a customer, this is done on the basis of a corresponding agreement for order processing in accordance with Art. 28 GDPR.

11. E-mail Communication

11.1 Contractually or technically required e-mails

11.1.1 In connection with an SF2 user account, an order, a download, or a license, we send emails that are necessary for the functions requested by the user, the execution of a contract, the license provision, or the security of the user account and the provided software. This particularly includes email confirmations, user account and security messages, password reset messages, order and contract confirmations, billing and payment information, messages regarding license activation, the provision of license files, notices of the impending expiration of temporary licenses, as well as legally or contractually required update and security information.

11.1.2 For this purpose, we process in particular the email address as well as the user account, contract, order, or license data required for the respective message and, if applicable, technical dispatch and delivery information.

11.1.3 The legal basis is Art. 6 Para. 1 lit. b GDPR. Security-relevant notifications can additionally be based on Art. 6 Para. 1 lit. f GDPR.

11.1.4 Contractually or technically necessary emails are separated from voluntary email information. In particular, the sending of legally or contractually required security and update information, license notifications, or other messages necessary for the execution of the contract or safety does not depend on consent to product information or company communications.

11.2 Voluntary SF2 Product Information

11.2.1 If you activate the corresponding setting, we will inform you by e-mail about SF2 products and product-related developments. This may include, in particular, information about software and hardware, new or updated software versions, features, editions, components, extensions, compatibilities, and other product updates.

11.2.2 The information may also relate to SF2 products that the recipient currently does not use or license. For this purpose, in particular, the e-mail address as well as the time, content, and status of the consent, and, if applicable, the user account identification are processed. Changes and revocations are also documented.

11.2.3 The legal basis is your voluntary consent pursuant to Art. 6(1)(a) GDPR in conjunction with § 174 TKG 2021.

11.3 SF2 News - Company News

11.3.1 If you activate the corresponding setting, we will inform you by e-mail about news from SF2 Systems. This may include, in particular, information about projects, events, case studies, collaborations, and other company developments.

11.3.2 In particular, your e-mail address as well as the time, content, and status of the consent and, if applicable, the user account identification are processed. The legal basis is Art. 6(1)(a) GDPR in conjunction with § 174 TKG 2021.

11.4 Management and Revocation

11.4.1 The consents for SF2 product information and SF2 news are independent of each other and can each be granted or revoked separately.

11.4.2 Users with an SF2 user account can change their settings at any time under "Subscriptions & Notifications." If an email contains an unsubscribe link, consent can also be revoked directly via this link; this applies in particular to recipients without an SF2 user account.

11.4.3 The revocation takes effect for the future and does not affect the legality of processing carried out up to the point of revocation. Records of previously given consent can be retained after the revocation as long as this is necessary to fulfill legal proof obligations or to assert, exercise, or defend possible legal claims.

11.4.4 The termination of a license is independent of voluntary email settings. Similarly, the revocation of email consent does not lead to the termination of an existing license.

12. Cookies and comparable technologies

12.1 Technically necessary technologies

12.1.1 Our website and the associated online services use cookies and comparable technologies, insofar as these are necessary for the operation of the website or you have consented to their use.

12.1.2 Technically necessary technologies are used in particular to maintain login sessions, securely authenticate users, protect forms and activation processes, prevent unauthorized access and cross-site request forgery attacks, store privacy and cookie settings, and provide explicitly requested functions.

12.1.3 To the extent that storing information on your device or accessing already stored information is strictly necessary to provide a function you have explicitly requested or to enable the transmission of a message, no prior consent is required for this in accordance with § 165 para. 3 TKG 2021. If personal data is processed in this context, this is done depending on the purpose, in particular on the basis of Art. 6 para. 1 lit. b or lit. f GDPR.

12.2 Consent management with KLARO!

12.2.1 To manage your consents for optional cookies and similar technologies, we use KLARO!. The system is operated locally by us and serves to record your selections, store them, and take them into account during further visits.

12.2.2 Through the link "Cookie Settings" in the footer of our website, you can view and change your selection at any time, as well as revoke a consent already given with effect for the future. There you will also find an up-to-date overview of the cookies and similar technologies used, including a) Name; b) Provider; c) Purpose; d) Category; and e) Storage duration.

12.3 Website Analysis with Matomo

12.3.1 We use Matomo to statistically analyze the use of our website and to improve our website, content, user guidance, and technical processes. Matomo is only activated after you have consented to the use of the corresponding analysis technologies via KLARO!. Without such consent, no optional Matomo analysis takes place.

12.3.2 With analysis enabled, depending on the technical configuration, the following information in particular can be processed: a) IP address in shortened or anonymized form; b) pages and content accessed; c) date and time of page visits; d) origin or referrer; e) browser type and browser version; f) operating system; g) device and display information; h) language settings; i) visit and session information; j) duration of stay; and k) interactions with our website.

12.3.3 The legal basis is your consent pursuant to Art. 6 para. 1 lit. a GDPR in conjunction with § 165 para. 3 TKG 2021.

12.3.4 Matomo is operated by SF2 Systems itself; the analysis is carried out according to the current system configuration at the location in Germany. Analysis data is only stored as long as it is necessary for statistical evaluation and improvement of our website, and is then deleted or anonymized. The storage duration of the cookies or comparable technologies used on your device is specified in the cookie settings.

12.3.5 Consent can be revoked at any time via the cookie settings with effect for the future. After a revocation, the optional Matomo analysis will no longer be activated for the respective user.

13. Technical infrastructure, service providers, and recipients

13.1 Recipient categories

13.1.1 As far as this is necessary for the in this Privacy Policy Personal data may, if necessary for the purposes described, in particular be transmitted to or processed by the following recipients or categories of recipients: a) providers of hosting and IT infrastructure services; b) providers for email dispatch and delivery; c) payment service providers; d) IT security, maintenance, and technical support service providers; e) tax advisors; f) legal advisors and other professional consultants; and g) authorities and courts, insofar as there is a legal obligation to disclose or the transfer is necessary for asserting, exercising, or defending legal claims.

13.2 Processors and independent controllers

13.2.1 Insofar as external service providers process personal data exclusively on our behalf, they are used as processors. With them, we conclude agreements in accordance with Art. 28 GDPR, insofar as legally required. We only select such processors who provide sufficient guarantees for data protection-compliant processing.

13.2.2 Insofar as a recipient processes personal data for their own purposes and under their own data protection responsibility, the transfer takes place on the basis of the respective applicable data protection provisions. This particularly concerns Mollie in the context of payment processing.

13.3 Systems used and processing locations

13.3.1 According to the current system configuration, the following services are used in particular:

a) Technical infrastructure - location Germany;

b) SF2 user account and authentication - in-house operation, location Germany;

c) Website analysis with Matomo - in-house operation, location Germany;

d) License system - in-house operation, location Germany;

e) Consent management with KLARO! - in-house operation, location Germany;

f) Email delivery - Fastmail Pty Ltd, location Australia as well as

g) Payment processing - Mollie B.V., Netherlands.

14. Transmission of personal data to third countries

14.1 General requirements

14.1.1 Insofar as personal data is transferred to recipients outside the European Union or the European Economic Product preview, this is done exclusively in compliance with Articles 44 et seq. of the GDPR.

14.1.2 Such a transfer may in particular be based on an adequacy decision of the European Commission pursuant to Article 45 GDPR, on appropriate safeguards such as the standard contractual clauses of the European Commission pursuant to Article 46 GDPR, or on another transmission basis permissible under the GDPR.

14.2 Email transmission to Australia

14.2.1 For email dispatch, we use Fastmail Pty Ltd, Australia. As part of the service provision, the processing of personal data may also take place outside the European Economic Product preview. To the extent that no adequacy decision by the European Commission exists for such a transfer, it is carried out on the basis of appropriate safeguards, in particular the standard contractual clauses pursuant to Art. 46 Para. 2 lit. c GDPR.

14.2.2 Further information on the safeguards used in connection with transfers to third countries can be requested at info@sf2systems.com .

15. Provision of personal data

15.1 Required and voluntary information

15.1.1 The provision of certain personal data is necessary for us to provide the services requested by the user or to perform a contract. Without a valid email address, for example, no SF2 user account can be created and no email confirmation can be carried out.

15.1.2 For the creation of a device-bound license, technical information about the licensed target system, in particular a hardware ID, may be required. For paid orders, the information necessary for concluding the contract, invoicing, and payment processing must be provided.

15.1.3 Mandatory fields are marked accordingly in the respective forms. Any information beyond this is voluntary, unless expressly stated otherwise.

15.1.4 If required information is not provided, the respective service cannot be provided or cannot be provided in full. In particular, a paid order cannot be processed without the information required for contract conclusion, invoicing, and payment processing, and a device-bound license cannot be issued without a hardware ID.

16. Retention period

16.1 General principles

16.1.1 Unless a specific retention period is mentioned in this Privacy Policy document, we only store personal data as long as it is necessary for the respective processing purpose.

16.1.2 Any further storage takes place in particular if a) legal retention obligations exist; b) a contractual or licensing relationship continues; c) data is required for documenting existing rights or consents; d) the data is needed to assert, exercise, or defend legal claims; or e) a specific case of security, fraud, or misuse is being investigated.

16.1.3 After the respective purpose of processing ceases and existing statutory retention or limitation periods have expired, personal data is deleted or, to the extent permissible and appropriate, anonymized.

17. Automated Decision-Making

17.1 No automated decisions within the meaning of Art. 22 GDPR

17.1.1 SF2 Systems does not use exclusively automated decision-making processes in connection with the website, SF2 user accounts, downloads, orders, and license activations, which have legal effects for the affected persons or similarly significantly affect them.

17.1.2 The automated technical creation, signing, or provision of a license file does not in itself constitute an automated evaluation of personal aspects or profiling in the sense of such decision-making.

18. Rights of affected individuals

18.1 General rights

18.1.1 Under the legal conditions, data subjects in particular have the following rights: a) Right of access in accordance with Art. 15 GDPR; b) Right to rectification in accordance with Art. 16 GDPR; c) Right to erasure in accordance with Art. 17 GDPR; d) Right to restriction of processing in accordance with Art. 18 GDPR; e) Right to data portability in accordance with Art. 20 GDPR; f) Right to object in accordance with Art. 21 GDPR; and g) Right to withdraw given consent with effect for the future.

18.2 Objection and withdrawal

18.2.1 Insofar as we process personal data on the basis of Art. 6(1)(f) GDPR, the data subject has the right to object to processing at any time for reasons arising from their particular situation. After such an objection, we will no longer process the relevant data unless we can demonstrate compelling legitimate grounds for processing that override the interests, rights, and freedoms of the data subject, or if the processing serves the establishment, exercise, or defense of legal claims.

18.2.2 If personal data is processed for the purposes of direct marketing, this processing can be objected to at any time. Following such an objection, the relevant data will no longer be used for direct marketing.

18.2.3 A given consent can be revoked at any time with effect for the future. The lawfulness of the processing carried out until the revocation remains unaffected.

18.3 Exercise of rights

18.3.1 To exercise your rights, you can contact us at info@sf2systems.com . To the extent necessary to protect personal data, we may request additional information to sufficiently verify the identity of the requesting person.

18.4 Separate notice on the right to object

Notice pursuant to Art. 21 para. 4 GDPR:

You have the right to object at any time to the processing of your personal data on grounds relating to your particular situation, which is carried out on the basis of Art. 6(1)(f) GDPR.

We will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing serves the establishment, exercise, or defense of legal claims.

If your personal data is processed for direct marketing purposes, you may object to this processing at any time and without giving reasons. After such an objection, your data will no longer be processed for these purposes.

You can submit your objection informally to info@sf2systems.com direct.

19. Right to lodge a complaint

19.1 Competent supervisory authority

19.1.1 If you believe that the processing of your personal data violates data protection regulations, you have the right to lodge a complaint with a competent data protection supervisory authority.

19.1.2 In Austria, this is:

Austrian Data Protection Authority
Barichgasse 40-42
1030 Vienna
Austria

Email: dsb@dsb.gv.at
Phone: +43 1 52 152-0

19.1.3 The right to contact another data protection supervisory authority competent under statutory provisions remains unaffected.

20. Data security

20.1 Technical and organizational measures

20.1.1 SF2 Systems takes appropriate technical and organizational measures to protect personal data from loss, accidental or unlawful alteration, unauthorized access, unauthorized disclosure, and other unlawful processing.

20.1.2 The measures are regularly reviewed and adjusted if necessary, taking into account the state of the art, implementation costs, as well as the nature, scope, circumstances, and purposes of the processing and the associated risks.

21. Changes to these Privacy Policy

21.1 Update

21.1.1 SF2 Systems adjusts these Privacy Policy when the website, the offered features, the technologies or service providers used, or the relevant legal frameworks change.

21.1.2 The current version is made available on our website. In the case of significant changes, further information will be provided, as far as legally required.