CRIF BÜRGEL
Together to the next level

Technische und organisatorische Maßnahmen

Technical and organisational measures

Information Datenschutz
Information on data security

TOMs_20180531_v1.0.0

Inhaltsverzeichnis
Content

Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen entsprechend dieser Anlage zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Der Auftragnehmer wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers gegen Missbrauch und Verlust treffen, die den Forderungen der DSGVO entsprechen.

Technical and organisational measures (TOM)

The contractor ensures for his area of responsibility the implementation of and abidance by technical and organisational measures agreed upon, according to this appendix. In particular, the contractor will design his internal organisation so as to be compliant with data protection requirements.

The contractor will implement appropriate technical and organisational measures to protect customer data from misuse or loss, according to the requirements of the GDPR.

Dies beinhaltet insbesondere:

This includes in particular:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Confidentiality (Article 32, paragraph 1, point (b) GDPR)

Zutrittskontrolle

Ziel: Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte

Für den Zutritt zu den Bürogebäuden von CRIFBÜRGEL ist ein Schlüssel erforderlich, der Zutritt zu den Büros selbst ist zusätzlich zur Schließung durch eine Chipkarte oder einen Passivtransponder gesichert. Vereinzelungsanlage, Alarmanlage, Wachdienst und Videoüberwachung sind weitere Komponenten zur Sicherung von Haupteingängen und Technikräumen.

Besucher werden an der Rezeption in Empfang genommen und dort von dem jeweiligen Fachbereich abgeholt. Die weitere Begehung ist betriebsfremden Personen nicht bzw. nur in Begleitung eines Mitarbeiters gestattet. Die einzelnen Bürobereiche sind nach Aufgabenbereichen strukturiert.

Access control

Objective: Denial of admittance to data-processing equipment for unauthorised persons

To enter CRIFBÜRGEL premises, a key is needed. An additional security card or passive transponder system is installed. Turnstiles, an alarm system, a security service and camera systems are additional components that secure CRIFBÜRGEL main entrances and technical rooms.

Visitors are welcomed at reception and are picked up by someone from the relevant department. Unauthorised persons are prohibited from walking through the premises on their own; however, they may be accompanied by a CRIFBÜRGEL employee. Office areas are structured according to areas of responsibility

Zutritt zu Technikräumen

In den Bürogebäuden liegende Technikräume sind zusätzlich durch Chipkarte und/oder PIN-Schlösser gesichert.

Access to engineering rooms

Engineering rooms are located inside our office buildings and are secured by a chip card system and/or PIN key locks.

Zutritt zum Rechenzentrum

Das Gebäude des Rechenzentrums ist von einem Sicherheitszaun umgeben, dessen Torschleuse sich nur mittels eines Chipkartenlesers/einer Chipkarte öffnen lässt. Das Gebäude wird außerdem durch Kameras und einen Wachdienst geschützt.
Der Zutritt zum Gebäude ist durch eine Alarmanlage und ein elektronisches Chipkartenschloss gesichert. Zutritt zu beiden Systemen ermöglichen eine gültige Chipkarte und zwei sechsstellige PINs (Schließ- und Alarmanlage). Die Chipkarte befindet sich in einem Tresor, zu dem nur bestimmte Mitarbeiter der IT-Infrastruktur Zugang haben. Jede Entnahme der Chipkarte wird dokumentiert. Die Liste der zutrittsberechtigten Personen wird regelmäßig überprüft und zeitnah aktualisiert, externes Wartungspersonal hat nur in Begleitung von berechtigten Personen Zutritt.

Access to the data centre

The Data centre premises are fenced; the lock gate can only be opened by a special chip card system. A camera system and our security service complete the security.

The entrance is secured by an alarm system, and the doors can only be opened with a chip card and a double PIN code. The special chip card is stored in a safe, and only authorised people from the IT operations department have access to it. Each removal of the chip card is documented. The list of authorised people is reviewed on a regular basis and updated in a timely manner. External maintenance personnel can only enter the DC in the company of an authorised person.

Systemzugangskontrolle

Ziel: keine Nutzung der Datenverarbeitungsanlagen durch Unbefugte

Im gesamten CRIFBÜRGEL System ist keine Transaktion ohne gültige Authentifizierung und Autorisierung möglich. Der Zugang zu den Systemen wird durch mehrere Sicherheitsmechanismen abgesichert.

Der Zugang zu Systemen erfolgt durch Eingabe von Benutzername und Passwort, wobei das Passwort Restriktionen bzgl. Länge, Sonderzeichen etc. unterliegt.

Die Vergabe der Nutzerzugangsdaten erfolgt auf schriftlichen Antrag durch den HelpDesk. Nach erstmaligem Login muss das Passwort vom Nutzer geändert werden.

System access control

Objective: no access to data-processing systems by unauthorised persons

Without valid authentication and authorisation, no transaction is possible throughout the entire CRIFBÜRGEL data-processing system. Access to all systems is secured by several security measures.

Systems can only be accessed by entering a username and password, whereby the password is subject to restrictions regarding length, special characters, etc.

User access data is allocated upon written application by the HelpDesk. After the first login, the password has to be changed by the user.

Das Passwort muss außerdem durch den Benutzer regelmäßig geändert werden, eine wiederholte Verwendung desselben Passwortes wird durch das System unterbunden. Fehlerhafte Anmeldeversuche führen zur Sperrung des Benutzers, der nur nach Prüfung und durch den HelpDesk bei gleichzeitiger Vergabe eines neuen Passwortes wieder freigeschaltet wird.

In addition, the password must be changed regularly by the user; repeated use of the same password is prevented by the system. Incorrect login attempts lead to the blocking of the user, who will only be unblocked after verification and by the simultaneous assignment of a new password from the HelpDesk.

Das interne Netz (LAN) ist durch Virtual-Local-Area-Network-(VLAN-) Technologie in mehrere Segmente eingeteilt. Die Segmente sind u. a. Produktionssysteme, Testsysteme und Bürosysteme.

The internal local area network (LAN) is divided into several segments by virtual local area network (VLAN) technology. The segments include production systems, test systems and office systems.

Die Netzübergänge sind durch Firewallsysteme geschützt und werden überwacht. Unbenutzte LAN-Ports sind technisch gesperrt und werden nur kontrolliert in Betrieb gesetzt.
Der Übergang vom internen Netz zu Fremdnetzen (Internet, Partner- und Kundennetze) ist nur an zentralen Stellen möglich, die durch ein mehrstufiges Firewallsystem gesichert sind und sowohl von CRIFBÜRGEL als auch durch Dritte überwacht und regelmäßig geprüft werden (z. B. PEN-Test).

The gateways are protected by firewall systems and are monitored. Unused LAN ports are physically locked and only put into operation in a controlled manner.
The transition from the internal network to external networks (Internet, partner networks or customer networks) is only possible at central points, which are secured by a multilevel firewall system and monitored and regularly checked by both CRIFBÜRGEL and third parties (e.g. Pentest).

Zugriffskontrolle

Ziel: Zugriffsbeschränkung für Berechtigte, Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen von Daten

Allen Nutzern sind entsprechend Ihren Tätigkeiten bestimmte erforderliche Funktionen zugeordnet, die über den Benutzernamen gesteuert werden.
Die Einrichtung von Nutzern wird durch den HelpDesk durchgeführt. Die Nutzer erhalten vom HelpDesk Passwörter für den Zugang zu den Anwendungen, mit denen personenbezogene Daten verarbeitet werden. Im gesamten CRIFBÜRGEL System ist keine Transaktion ohne gültige Authentifizierung und Autorisierung möglich.

Data access control

Objective: Limited access for authorised users; protection against unauthorised reading, copying, modification or deletion of data

All users are assigned certain necessary functions according to their activities, which are controlled via their username.
Users receive passwords from the HelpDesk for accessing the applications that process personal data. Throughout the CRIFBÜRGEL system, no transaction is possible without valid authentication and authorisation.

Die Nutzer der Anwendungen haben nur in dem für die konkrete Rolle erforderlichen Umfang Zugriff auf personenbezogene Daten (Need-to-know-Prinzip). Ergänzend werden Daten und Dokumente, soweit geboten und technisch möglich, verschlüsselt gespeichert und übertragen.

The users of the applications have access to personal data only to the extent required for the specific role (need-to-know principle). In addition, data and documents are stored and transmitted in an encrypted form as far as necessary and technically possible.

Damit sind unerlaubte Tätigkeiten in CRIFBÜRGEL Systemen außerhalb eingeräumter Berechtigungen verhindert und eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung ist gegeben.

This prevents unauthorised activities in CRIFBÜRGEL systems outside of granted authorisations, and provides a demand-oriented design of the authorisation concept and the access rights, as well as their monitoring and logging.

Trennungskontrolle

Separation control

Ziel: Zweckgebundenheit der Datenverarbeitung sicherstellen

Objective: Ensuring the appropriateness of the data processing

Der Datenzugriff ist nur anhand von Berechtigungskonzepten möglich. Datenzugriff ist nur für die jeweils erforderlichen Zwecke möglich. Die Datenbestände der betriebenen Anwendungen werden getrennt voneinander betrieben, sodass aus einer Anwendung kein Zugriff auf andere Anwendungen möglich ist.

Data access is only possible using authorisation concepts. Data access is only possible for the purposes required. The databases of the operated applications are operated separately so that one application cannot access other applications.

Jeder Einmelder und jeder eingelesene Datensatz ist eindeutig über eine Referenznummer identifizierbar. Jeder Zugriff über die Produkte auf die Daten ist eindeutig identifizierbar und nachvollziehbar. Transaktionen werden separat geloggt.

Every external data input and each read-in data is clearly identifiable by a reference number. Every access to the data via the products is clearly identifiable and traceable. Transactions are logged separately.

Kundendatenbestände werden auf der Basis jeweils eigener Kunden-Accounts logisch voneinander getrennt. Dabei ist die Mandantenfähigkeit der eingesetzten IT-Systeme gegeben. Die zu unterschiedlichen Zwecken erhobenen Daten werden auch getrennt verarbeitet.

Customer data is separated logically based on individual customer accounts. The multi-client capability of the IT systems used is mandated. The data collected for different purposes is also processed separately.

Bei Betrieb einer Multiauskunfteistrategie des Kunden auf der CRIFBÜRGEL CSP Plattform:

When operating a customer's multi-credit-reporting strategy on the CRIFBÜRGEL CSP platform:

- CRIFBÜRGEL kann eine Anfrage jederzeit bedienen, auch wenn eine Quelle abgeschaltet ist.
- CRIFBÜRGEL is able to answer a request at any time, even if an external source is not available.

- CRIFBÜRGEL kann jede genutzte Datenquelle auch getrennt beauskunften, weil jede Quelle und/ oder Anfrage eindeutig referenziert wird.
- Die Herkunft der Daten ist jederzeit nachvollziehbar, d. h. wann von wem zu welchem Zweck Daten erhoben und gespeichert wurden.
- Transaktionsdaten sind vom eigenen Datenbestand separiert und werden nicht verändert oder zu einem anderen Zweck verwendet.

Eigene CRIFBÜRGEL Bestandsdaten und Daten von fremden Auskunfteien sind in den Transaktionsdaten immer und jederzeit eindeutig identifizierbar.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Ziel: Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen sowie Nachvollziehbarkeit erfolgter Übertragungen von Daten

Der Zugriff auf die Datenbanken erfolgt durch die Nutzer zum einen via FTP mit Tunnel/SFTP, zum anderen via Webservices, die über HTTPS abgesichert sind. Dabei wird nicht nur die Authentifizierung, sondern auch die Übertragung der Daten gesichert. In Absprache mit den Kunden und je nach Schutzbedarf der Daten wird eine Vielzahl von aktuellen Verschlüsselungsverfahren angeboten.

Jede Auskunftsanforderung wird im System registriert, sodass jederzeit geprüft werden kann, welche Daten von wem gespeichert, verarbeitet oder übermittelt worden sind. Ebenso kann der Empfänger einer Datenübermittlung ermittelt werden. Die Weitergabe von personenbezogenen Daten erfolgt bei direkter Anbindung prinzipiell verschlüsselt. Im Standard erfolgt die Kommunikation mit externen Clients immer verschlüsselt über HTTPS (HyperText Transfer Protocol Secure, sicheres Hypertext-Übertragungsprotokoll) und/oder VPN (Virtual Private Network). Die Übermittlung der Daten per E-Mail (SMTP) erfolgt PGP-verschlüsselt.
Für den Transfer von Dateien ist SFTP (Secure File

- CRIFBÜRGEL is able to provide inquiry information for any used data source separately because every source and/or inquiry is referenced.
- The origin of the data is traceable at any time, in particular when, why and by whom the data was collected and saved.
- Transaction data is kept separate from the personal data pool, and is not modified or used for another purpose.

Data belonging to CRIFBÜRGEL and data provided by external information bureaus as part of the transaction data are at any time clearly identifiable.

2. Integrity (Article 32, paragraph 1, point (b) GDPR)

Transfer control

Objective: Protecting personal data from unauthorised reading, copying, changing or deletion, and ensuring traceability of data transfer operations

Access to the database is granted to the user via FTP (file transfer protocol) with tunnel/SFTP (secure file transfer protocol), or via Web services secured by HTTPS (Hypertext Transfer Protocol Secure). Both the authentication and the transmission of the data is saved. In consultation with the customers and depending on the protection requirements of the data, a variety of state-of-the-art encryption methods are offered.
Each request for information is logged in the system in such a way that it can be checked at any time what data has been stored, processed or transmitted by whom. Likewise, the recipient of a data transmission can be determined. When personal data is transferred via direct connection, it is encrypted as a general rule. As standard, communication with external clients is encrypted using HTTPS and/or VPN (virtual private network). The transmission of the data by email (SMTP) is PGP-encrypted. File transfer requires SFTP or file encryption.

Transfer Protocol) oder eine Dateiverschlüsselung notwendig.
Ausrangierte Computerhardware, Datenträger und nicht mehr benötigte Unterlagen und Listenausdrucke werden durch einen Entsorgungsfachbetrieb zerstört. Die Geräte werden in einem abschließbaren, dedizierten Datenbehälter abtransportiert und fachgerecht entsorgt. Die Vernichtung wird protokolliert. Das Protokoll wird CRIFBÜRGEL zur Verfügung gestellt.

Certified disposal operations destroy discarded computer hardware, data carriers and unnecessary documents and printouts of lists. The devices are carried away in a dedicated lockable data container and disposed of properly. The destruction is logged and the protocol is made available to CRIFBÜRGEL.

Eingabekontrolle

Ziel: Nachvollziehbarkeit von Eingaben, Änderungen oder Löschung von Daten

Die Eingabe von Daten erfolgt in automatisierten Prozessen. Diese werden vorab in Testsystemen überprüft und unterliegen einem standardisierten Freigabeprozess. In diesen Prozessen wird jede automatisierte Eingabe protokolliert und ist jederzeit durch die eindeutige Prozess- und Transaktions-ID nachvollziehbar.

Durch die Protokollierung der Eingabedaten ist es jederzeit möglich, den ursprünglichen Zustand wiederherzustellen.

Auf Basis eines Rollen- und Rechtekonzepts werden den Mitarbeitern von CRIFBÜRGEL in Abhängigkeit ihrer Funktion und der zu bearbeitenden Datenbestände differenzierte Berechtigungen zugewiesen. Die Verarbeitung von Daten durch die Mitarbeiter wird protokolliert.

Manuelle Einzeleingaben erfolgen über eine Programmebene, die ebenfalls benutzerbezogen die einzelnen Schritte und Aktivitäten des Anwenders protokolliert. Das Eingabeprogramm unterliegt ebenfalls dem standardisierten Freigabeprozess von CRIFBÜRGEL.

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, sind im Einsatz.

Input control

Objective: Traceability of entries; changes to or deletion of data

Data is inputted via automated processes. These are checked in advance in test systems and are subject to a standardised approval process. In these processes, every automated input is logged and is traceable at any time by the unique process and transaction ID.

Using the input data log, it is possible to restore the original state at any time.

Based on a role and rights concept, CRIFBÜRGEL employees are assigned different authorisations depending on their function and the data records to be processed. The processing of data by employees is logged.

Individual entries made manually are done through a program that logs the individual steps and activities of the specific user. The input program is also subject to the standardised approval process at CRIFBÜRGEL.

The traceability and documentation of data management and maintenance is guaranteed. Measures for the subsequent verification of whether and by whom data has been entered, changed or deleted are in place.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Ziel: Schutz vor Datenverlust und Datenwiederherstellung in angemessener Zeit

Die Verfügbarkeit der produktiven Daten wird durch die eingesetzten Betriebstechniken (u. a. Storage Area Network [SAN], Virtualisierung und Spiegelung) und die Datensicherung gewährleistet.
Netzwerkkomponenten (z. B. NIC, Switches) und Carrier-Verbindungen (WAN) sind redundant ausgelegt und mit Servicevereinbarungen (SLA/UC) gestützt. Komponenten und Verbindungen werden durch CRIFBÜRGEL und durch Dritte (z. B. Provider) überwacht.

In der Produktion sind alle Server doppelt oder mehrfach vorhanden. Im Falle eines Ausfalls wird (automatisiert) der jeweils andere Server eingesetzt. Durch Virtualisierung ist eine schnelle Bereitstellung gewährleistet. Das Transaktionslog der produktiven Datenbanken erlaubt auch im Falle eines Ausfalls mit Datenverlust eine Wiederherstellung des Produktionssystems.

Die Datensicherung erfolgt zusätzlich mehrfach über Magnetbandlaufwerke. Die Magnetbänder werden sowohl onsite vorgehalten als auch ausgelagert. Rücksicherungen auf Band werden regelmäßig getestet (Stichproben, automatisiert).

CRIFBÜRGEL betreibt zusätzlich ein Notfallrechenzentrum (Geo-Redundanz), in dem alle produktiven Daten vorgehalten werden.

Maßnahmen zum Schutz vor Schäden durch Feuer und Wasser sind in den dezentralen Technikräumen installiert. Alle für die Produktion relevanten Datenbestände werden zentral im Rechenzentrum vorgehalten.

3. Availability and resilience (Article 32, paragraph 1, point (b) GDPR)

Availability control

Objective: Data loss prevention and data recovery in a timely manner

The availability of productive data is ensured by the operating techniques used (including storage area network (SAN), virtualisation and mirroring) and data backup.
Network components such as NICs or switches and carrier connectivity are configured redundantly, and supported by service level agreements (SLA/UC). Both components and connections are monitored by providers and by CRIFBÜRGEL.

In production, all servers are available twice or more. In the event of a failure, the other server is automatically used. Virtualisation ensures fast deployment. The transaction log of the productive databases also allows for the recovery of the production system in the event of a failure with data loss.

In addition, data is backed up several times on magnetic tape drives. Tape cartridges are held both on-site and off-site, in secure locations. Restoring and retrieval are tested on a regular basis (spot checks, automated).

CRIFBÜRGEL also runs an emergency data centre (geo-redundancy), where all production services are available.

Protective measures against damage caused by fire and water are installed in the decentralised technical rooms. All databases relevant to production are stored centrally in the data centre.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Auftragskontrolle

Ziel: ausschließliche auftragsbezogene Verarbeitung der Daten

Auftragserteilung und Auftragsbearbeitung erfolgen bei CRIFBÜRGEL mittels Standardprozessen. Die für die Geschäftsfelder „Risk“, „Solutions“ und „Recovery“ einschlägige Auftragsverarbeitung wird durch CRIFBÜRGEL als Auftragsverarbeiter schriftlich dokumentiert.

Datenerhebung

Im Rahmen der automatisierten Datenerhebung werden die Aufträge (Einmeldungen) mit einem sogenannten Bearbeitungsstatus per Datei eingeliefert. Der Einmelder ist eindeutig per Referenz identifizierbar. Jede Datei und jede Einmeldung erhält eine eindeutige ID.

Entsprechend des Bearbeitungsstatus des Einmelders handelt es sich um

1. eine Neuanlage,
2. einen Löschauftrag oder
3. eine Aktualisierung.

Die einzelnen Aufträge werden historisiert abgelegt. Daten werden immer in den für den Zweck vorgesehenen Tabellen gespeichert.

Beauskunftung

Anfragen des Kunden werden über Produkte durchgeführt. Die Produkte werden entsprechend dem Vertrag mit dem Kunden zweckgebunden konfiguriert. Jede Anfrage durch den Kunden wird nur im Kundenkontext durchgeführt.

4. Regular review, assessment and evaluation procedures (Article 32, paragraph 1, point (d) GDPR)

Order control

Objective: Exclusively order-related data processing

Orders placed and processed at CRIFBÜRGEL use standard processes. The order processing relevant to the business areas ‘Risk’, ‘Solutions’ and ‘Recovery’ is documented in writing by CRIFBÜRGEL as the processor.

Data collection

As part of the automated data collection, the orders (Einmeldungen) with a so-called processing status are delivered by files. The customer is clearly identifiable by reference. Each file and message receives a unique ID.

Depending on its processing status, the order represents a:

1. new entry,
2. an order to delete, or
3. an update.

The individual orders are stored in the history. Data is always stored in the tables provided for this purpose.

Provision of information

Inquiries from the customer are processed via products. The products are configured according to the contract with the customer. Each inquiry by the customer is made only within the customer context.

Die dabei übermittelten Daten von externen Auskunfteien werden nicht für etwaige andere Beauskunftungen erneut verwendet. Es ist über eine eindeutige Referenzierung in den Logs immer nachvollziehbar, welche Daten für welche Anfrageaufträge beauskunftet wurden.

The data transmitted from external credit bureaus will not be reused for any other provision of information. Using a unique reference system in the logs, it is possible to trace at any time what data was provided for which requests orders.

Die weisungsgemäße Auftragsverarbeitung ist gewährleistet und Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind gegeben.

The processing of orders in accordance with instructions is guaranteed, and the measures (technical/organisational) to delimit the authorisations between the client and the contractor are mandated.

5. Sonstiges

Überwachung durch die Aufsichtsbehörde

CRIFBÜRGEL unterliegt aufgrund seiner Tätigkeit als Auskunftei der regelmäßigen Überprüfung der zuständigen Aufsichtsbehörde. Für CRIFBÜRGEL ist das Bayerische Landesamt für Datenschutzaufsicht zuständig.

Verpflichtung der Mitarbeiter auf das Datengeheimnis, Sicherheitsrichtlinie

Der Datenschutzbeauftragte schult und überwacht die Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Vorschriften. Sämtliche an der Datenverarbeitung beteiligten Mitarbeiter sind über die datenschutzrechtlichen Anforderungen unterrichtet. Eine Verpflichtungserklärung über das Datengeheimnis liegt für jeden Mitarbeiter vor.

Des Weiteren werden die Mitarbeiter von CRIFBÜRGEL durch eine interne Sicherheitsrichtlinie, die verbindlich zu unterzeichnen und einzuhalten ist, an interne Sicherheitsstandards gebunden.

5. Miscellaneous

Monitoring by the supervisory authority

CRIFBÜRGEL is subject to regular reviews by the competent authority due to its activity as a credit bureau. For CRIFBÜRGEL, the Bavarian State Office for Data Protection Supervision is in charge.

Commitment of employees to data secrecy; security policy

The data protection officer trains and monitors employees for compliance with data protection regulations. All employees involved in data processing are informed about the data protection requirements. A formal commitment to data secrecy exists for each employee.

Furthermore, the employees of CRIFBÜRGEL are bound by an internal security policy, which must be signed and adhered to, in accordance with internal security standards.