Service Description

General

DataCo offers services for the independent support of the Customer's management in the areas of data privacy, information security and compliance.
DataCo's services are designed to improve the protection of persons affected by potential rights violations and relates to a professional assessment of the Customer's technical and organisational preventative measures.
This service does not constitute any form of legal advice but relates solely to the professional support of the Customer with regard to the organisation, documentation and automation of its processes to ensure data privacy, information security and compliance with due regard to applicable legal provisions, standards and best practices.
For this purpose, the Customer's coordinators will inform DataCo and present DataCo with the relevant issues that fall under the scope of the contractual services.
DataCo reports to the management of its customers from an unbiased position.

The Customer bears the sole management responsibility for data privacy, information security and compliance as well as the operative implementation of DataCo's independently prepared recommendations for action.
The business hours of the DataCo are weekdays (Monday to Friday) from 9:00 to 17:00 hours.
Unless agreed otherwise, all services will be provided in English.
Only those items of the service description which the Customer has expressly ordered will be part of the Customer's individual service scope. In terms of technical requirements for the provision of the services, the Customer must have internet access and an up-to-date internet browser.
The Contract does not cover the provision of equipment or services to meet these technical requirements.

The Web-Based DataCo Platform (hereinafter referred to as "DataGuard Platform") promotes the exchange of information through the digitisation, automation and documentation. The "Special terms of use DataGuard Platform" apply to the use of the Platform. The Platform users appointed by the Customer will receive access to the DataGuard Platform with the contents from the respective booked areas of data protection, information security and compliance via a digital invitation. The DataGuard Platform is provided to the Customer in one language; language options are currently limited to English and German. The DataGuard Platform serves as the central source of information to avoid time-consuming and repetitive tasks, while simplifying the communication between the Customer and DataCo.

There is no obligation for the DataGuard Platform to be always available. Whilst DataCo shall use all reasonable endeavours to make the DataGuard Platform available, DataCo shall have no liability if the DataGuard Platform is not available. During outages of the DataGuard Platform as a result of (software) maintenance, particularly planned periods of unavailability, as well as periods during which the data privacy platform is not available as a result of technical or other problems which do not fall within the scope of influence of DataCo (e.g. force majeure, culpability of third parties, etc.), the service obligations will be suspended accordingly. Any unavailability of the DataGuard Platform, or any failure of operation relating to the DataGuard Platform, shall be reported by the Customer and DataCo shall use its reasonable endeavours to remedy the defect within an appropriate period. At the end of the Contract, Customer access to the DataGuard Platform will be blocked; the Customer must ensure a back-up of all data on their systems before said date.

Privacy Area

Privacy Audit

The Privacy Audit is an initial assessment of the Customer's processing operations. It shall be carried out with the Customer, digitally and over the phone. The data privacy audit is binding on initial commissioning by the Customer and constitutes an essential foundation for the provision of the service. The points of contact designated by the Customer shall respond to the questionnaires on processing operations stored on the DataGuard Platform. The resulting information will be evaluated by DataCo. Afterwards, the DataCo Privacy Team will carry out the audit calls with the points of contact of the Customer. The Customer shall ensure that the points of contact who participate in the calls are correspondingly qualified to provide information on all topics of the audit in question. The information provided by the Customer during the data privacy audit helps DataCo to generate recommended actions to improve the protection of personal data and advance the Customer's compliance with data protection regulations. The Customer bears the sole obligation and responsibility to implement these recommendations at all times.

Appointment as Data Protection Officer (DPO) and data protection documentation with Records of Processing Activities (RoPA) and Technical and Organisational Measures for data protection (TOMs)

This service item includes (1) the appointment of DataCo as Data Protection Officer (DPO) and submission of notification hereof, (2) initial generation of data privacy documentation and (3) regular data privacy updates..

1. The Customer appoints DataCo as its external DPO. If permissible, DataCo will notify the supervisory authority competent for the Customer of its appointment as the DPO, with the Managing Directors specified in the Contract as the point of contact and will inform the Customer of said notification. If the authority requests a notification form, requiring the Customer to notify the authority by themselves, DataCo shall provide the Customer with the link to the relevant web portal of the authority. The Customer shall then notify the authority themselves, with the support of DataCo. On termination of the Contract, the Customer undertakes to immediately inform the competent supervisory authority of the dismissal of DataCo as the DPO, together with information on the appointment of the future DPO. As appointed DPO, DataCo will fulfil the legal obligations of a DPO in accordance with Art. 39 GDPR, which is defined as an independent monitoring and controlling function with extensive rights.
2. The information provided by the Customer during the data privacy audit is used as a foundation to generate the Record of Processing Activities (RoPA) and Technical and Organisational measures (TOMs) for the protection of personal data, in cooperation with the Customer. Audit logs of the answers are also generated.
3. DataCo will regularly inform the Customer of select technical and regulatory developments in the field of data protection by means of a regular data privacy update.

DataGuard Platform (Privacy Area)

The data privacy area of the DataGuard Platform offers a detailed overview of the progress of the audit on personal data processing operations, allows for the processing of prioritised recommended actions, uses automation processes to simplify the creation, processing, and updating of data protection documentation, contains a dashboard for the storage and downloading of data privacy documentation, provides the Customer with data privacy-relevant templates, contains a news dashboard for easy access to news on data protection topics, simplifies contact with the DataCo Privacy Team through a form for consulting requests, and supports platform users with an interactive Platform Guide. The Privacy Area of the DataGuard Platform contains questionnaires on the various standard processes (Procurement, Sales, Finance, HR, and IT & Security) and Core Processes. The latter comprise the industry-specific and company-specific data processing activities, with different characteristics for industrial enterprises, consulting companies, IT companies, hotel companies, trade companies, medical technology companies, public institutions, and other industries.

The Privacy Area of the DataGuard Platform provides access to the Privacy Policy Generator. A point of contact of the Customer can request access to the Privacy Policy Generator for select employees; the scope of services comprises the exact number of usage rights matching the number of employees specified in the Contract. A privacy policy is provided to the Customer in plain text and in the form of HTML code, for integration into the Customer's website, based on information provided by the Customer about plugins used on the website (e.g. Google Maps, Webfonts), technologies used on the website (e.g. hosting, content delivery networks), as well as other important information. The same applies to the option for creating privacy policies for Customer web shops, Facebook fan pages, forums, apps, and platforms. If the Customer requires support in the creation of privacy policies with the Privacy Policy Generator, this support is granted within the framework of the Consulting Hours for Individual Usage; the same applies to a final inspection of the privacy policies created by the Customer.

Privacy Training Courses

DataGuard Platform users designated by the Customer grant access to the Academy users, who receive access to digital training modules. The scope of services comprises the exact number of usage rights matching the number of employees specified in the Contract. Three tiers are available: basic training (privacy basic), advanced training (courses for specialised topics), and additional compliance training (infosec basic). The contents of the basic training modules lay the foundation for the protection and handling of personal data as required by the GDPR. After completing each course, Academy users can take a test covering the content they have just learned. After successfully passing the test, Academy users receive a certificate. After failing a test, they can run through the course and test again. All academy users receive individual access data. Access data may not be passed on to other persons or third parties. The Customer shall correspondingly require Academy users to maintain confidentiality on the access data. Internet access, a working email address and an up-to-date Internet browser are the technical requirements the Academy users must have for participation in training courses. Provision or transfer of these technical requirements do not form part of this Contract. The "Special terms of use DataGuard Academy" apply.

Privacy Check-Ins, p.a.

Privacy Check-Ins are provided in two formats: (1) Business Check-Ins and (2) Operational Check-Ins. If the Customer has just one Check-In included in the Contract, a Business Check-In is carried out. The agenda for each check-in is prepared by DataCo in advance. Privacy Check-Ins provide much needed evaluations and progress reviews of data privacy recommendations to help ensure ongoing privacy compliance. Preparation for the check-in and the time to conclude the check-in with the Customer are not taken from the designated Consulting Hours. Any follow-up actions or tasks from the Check-In must be taken from the designated Consulting Hours.

1. During the Business Check-In, an annual activity report from the DPO is provided to management. The annual activity report is provided once a year as per the contract start date. This report details the services DataCo performed in the previous 12 months to work towards compliance of the Customer with the data privacy regulations.
2. During Operational Check-Ins, DataCo carries out a 30-minute phone call with the Customer, during which the implementation status of recommended actions is discussed, taking current development into consideration. Updates to data privacy documentation are also completed as a result of recommendations being implemented.

Consulting Hours (max. per month / year)

The Customer will receive individual support from the DataCo Privacy Team, within the framework of the consulting hours included in the service, during the business hours stated above. The consulting hours included in the Contract are the maximum amount that the Customer is estimated to need; using less than the stated number of consulting hours will often be sufficient. Consultation is provided to the Customer in one language; language options are currently limited to English and German. Consulting hours may be used for following tasks: Creation and reviews of Data Processing Agreements (DPAs); reviews of Joint Controllership Agreements (JCAs); assistance with template creation; support with data subject requests; support with data breaches and the corresponding communication support with affected parties and the authorities; support with transparency and obligations to provide information; creation and reviews of new privacy policies; advice on the technical implementation of privacy (privacy by design & default); reviews of data privacy documentations; Data Protection Impact Assessments (DPIAs); advice on customer training on data protection obligations. If required, additional consulting hours are charged at the rates set out in the Contract.

Unused consulting hours expire without replacement at the end of the respective contractual year, unless a transfer of hours has been expressly agreed.

If a transfer of hours has been agreed with the option "from previous Year", unused consulting hours from the previous contractual year can be used within the first quarter of a contractual year, provided that the number of consulting hours used in the first quarter of the contractual year does not exceed half of the annual consulting hour quota. Consulting hours not used hereafter shall expire without replacement.

Insofar as a transfer of hours with the option "from previous year / next year" has been agreed, unused hours from the previous contractual year or the following contractual year can be used within a contractual year, insofar as the sum of the hours used in the contractual year does not exceed twice the annual quota of consulting hours. Consulting hours not used hereafter shall expire without replacement.

Cookie Manager

The software-based Cookie Manager (currently powered by Usercentrics) makes it possible to obtain and store website cookie consent and offers a customisable cookie banner with banner style options. The Cookie Manager offers explicit and implicit collection of consent and consent storage. The Customer has access to 20,000 monthly sessions, three domains and two languages (German and English). If the Customer requires more sessions, domains or languages, this can be inquired and granted directly through DataCo. If the agreed 20,000 monthly sessions are exceeded, a monthly surcharge of £8.00 per 10,000 sessions will apply and will automatically be invoiced by DataCo. An individual offer can be negotiated with DataCo starting at 500,000 sessions per month.

Only access to this service offering is provided via the DataGuard Platform. The specifications of the service provider, currently Usercentrics, apply to the scope of services and the Data Processing Agreement.

Portal for Data Subject Requests

The Portal for Data Subject Requests (DSRs) is an extension to the DataGuard Platform, adding functions that allow the management of data subject requests and the automatic recording of new enquiries. The portal comprises a website form for data subject requests with configuration options that can be embedded via a prefabricated html code on the Customer's website. Additionally, the portal includes a dashboard with workflow for the efficient management of data subject requests, and the option to request support from DataCo Privacy Team.

Portal for Privacy Partner Management

The portal for Privacy Partner Management is an extension to the data privacy platform, which offers visualisation options for the partner network and the relevant partner status, a template editor for the management of Data Processing Agreements (DPAs), simplifying the management of DPAs and Joint Controllership Agreements (JCAs), and offers the option of requesting a check of DPAs and JCAs, and enables inputs to create (and store) DPAs and JCAs.

DataGuard Badge

After successfully running through the Privacy Audit, and after DataCo deems a fundamental standard of data privacy to have been achieved through the creation of data privacy documentation and the implementation of recommended actions, the Customer will receive a DataGuard Badge, which they can use to represent their company to the outside world and highlight their collaboration with DataGuard in the field of data privacy. The DataGuard Badge does not serve as a proof of Data Protection compliance on the part of the Customer. Such proof can only be obtained from an independent and certified inspection body. Accordingly, the Customer undertakes to refrain from using the DataGuard Badge in its external representation in such a way as to suggest this constitutes said proof of compliance.

Erasure Concepts for Software Tools

When personal data are no longer necessary in relation to the purpose for which they were collected, it must be deleted. We support you with conceptualising erasure concept(s) for software tool(s) of your choice (e.g. Personio or MS Office), especially with evaluating, creating, or updating the erasure policy for data stored within this tool. This service pertains to software-based tools used by the Customer for the processing of personal data. This service is capped as per the maximum number of tools stated in the Contract. If the Customer requires erasure concepts for more tools than included in the Contract, they must individually book additional tools as an add-on.

Corporate Identity Branded Documentation

Documentation generated by the DataGuard Platform can be branded to match the Customer's corporate identity. Documentation which may be branded with corporate identity includes audit logs, RoPA and TOMs. Branding options are limited to adding Customer logo, adjusting font colours and adjusting fonts based on a pre-defined list. The Customer must provide all assets and information in the appropriate formats. Earliest availability of this function will be September 2022.

Enterprise Suite

The DataGuard Platform offers advanced functions for large organisations such as Single Sign-On (SSO), a corporate dashboard with overview of all entities, the capability to integrate the DataGuard platform to other software solutions and applications. These functions are in development and will be activated for the Customer upon request once released; earliest availability from April 2023. The Customer must provide any information required to facilitate set-up of these advanced functions. Integration capabilities are limited to those available within the DataGuard Integration Marketplace. DataGuard reserves the right to review Integrations usage annually and introduce additional fees for Integrations if the Customer exceeds standard usage limits.

Support and Platform in a Secondary Language

The DataGuard Platform (Privacy Area) as well as consultation from DataCo Privacy Team is available in multiple languages. Language options are currently limited to English and German. If multilingual support is requested, the DataGuard Platform (Privacy Area) can be made available in two languages; each language is accessed via a language switcher button within the DataGuard Platform. DataCo will ensure consultancy support is delivered in your chosen language by staffing a team to fit your requirements.

On-Site Visits

The Customer can request an on-site visit from a DataCo Privacy Team. Exact dates and times for the on-site visit must be coordinated between both the Customer and DataCo in advance. The maximum duration of an on-site visit is eight hours. The agenda and scope of tasks to be completed during the on-site visit must be coordinated and agreed between both the Customer and DataCo in advance. Travel expenses for the on-site visit are covered by the Customer. Each on-site visit is limited to visiting a single premises.

Information Security Area

Information Security Management System Gap Analysis

A gap analysis may be carried out in order to either (1) build a new Information Security Management System (ISMS), or (2) review an existing ISMS.

1. Following an onboarding and kick-off call, the Customer is given access to the DataGuard Platform, Information Security Area. The Customer will be provided with comprehensive questionnaires for the internal gap analysis, which covers all chapters of the Information Security Management System (ISMS). The points of contact designated by the Customer shall respond to the gap analysis questionnaires on processing operations stored on the web-based information security platform. The Customer shall ensure that the points of contact who participate in the calls are correspondingly qualified to provide information on all topics of the questionnaire in question. The resulting information will be evaluated by DataCo. Afterwards, the DataGuard Information Security Team will carry out evaluation calls with the points of contact of the Customer, in which DataCo will explain and identify needed ISMS chapters. Based on gap analysis, a list of prioritised recommendations (next steps) are generated. A gap analysis report for each of the ISMS chapters is also provided. All follow-up tasks to build the ISMS are billed from the Consulting Hours specified in the Contract.
2. Following an onboarding and kick-off call, the Customer is given access to the DataGuard Platform, Information Security Area. In addition, the Customer must provide all existing documentation to be verified and checked by DataCo to ensure that all relevant chapters of the ISMS are included. Based on the gap analysis, follow-up actions are defined. If any documentation is missing, the Customer must respond to the relevant gap analysis questionnaires on processing operations stored on the web-based information security platform, as explained above in point (1).

DataGuard Platform (Information Security Area)

The DataGuard Platform users named by the customer receive access to the contents of the Information Security Area via a digital invitation. This facilitates the exchange of information required to prepare and carry out the analysis of the customer’s information security processes, to prepare for an information security audit, and to help continually keep the Customer’s information security management system up to date.

The DataGuard Platform, Information Security Area offers detailed gap analysis questionnaires which cover all relevant chapters of the Customer’s information security management system (ISMS), allows for the processing of prioritised recommended actions, contains a dashboard for managing business assets, uses automation processes to simplify the creation of information security policies, and contains a dashboard for the storage and downloading of information security documentation. The gap analysis questionnaires contain seventeen questionnaires which cover all relevant chapters of the Customer’s information security management system.

InfoSec training courses

The DataGuard Platform users designated by the Customer grant access to the Academy users, who receive access to digital training modules. The scope of services comprises the exact number of usage rights matching the number of employees specified in the Contract. Three tiers are available: basic training (infosec basic), advanced training (courses for specialised topics), and additional compliance training (privacy basic). The contents of the basic training modules lay the foundation for the protection and handling of information as required by external certification auditors. After completing each course, Academy users can take a test covering the content they have just learned. After successfully passing the test, Academy users receive a certificate. After failing a test, they can run through the course and test again. All academy users receive individual access data. Access data may not be passed on to other persons or third parties. The Customer shall correspondingly require Academy users to maintain confidentiality on the access data. Internet access and an up-to-date Internet browser are the technical requirements the Academy users must have for participation in training courses. Provision or transfer of these technical requirements do not form part of this Contract. The “Special terms of use DataGuard Academy” apply.

InfoSec Check-Ins, p.a.

InfoSec Check-Ins are provided in two formats: (1) Business Check-Ins and (2) Operational Check-Ins. If the Customer has just one Check-In included in the Contract, a Business Check-In is carried out. The agenda for each check-in is prepared by DataCo in advance. InfoSec Check-Ins provide much needed evaluations and progress reviews of information security recommendations to help maintain a high-quality ISMS. Preparation for the check-in and the time to conclude the check-in with the Customer are not taken from the designated Consulting Hours. Any follow-up actions or tasks from the Check-In must be taken from the Consulting Hours.

During the Business Check-In, ISMS project status & a risk report is provided to management. This update is provided once a year as per the contract start date. This report details the services DataCo performed in the previous 12 months.
During Operational Check-Ins, DataCo carries out a 30-minute phone call with the Customer, during which the implementation status of recommended actions is discussed, taking current development into consideration. Updates to ISMS documentation and policies are also completed as a result of recommendations being implemented.

Consulting Hours (max. per month / year)

The Customer will receive individual support from the DataCo Information Security Team, within the framework of the consulting hours included in the service, during the business hours stated above. The consulting hours included in the Contract are the maximum amount that the Customer is estimated to need; using less than the stated number of consulting hours will often be sufficient. Consultation is provided to the Customer in one language; language options are currently limited to English and German. Consulting hours may be used for following tasks: Advice on updating and improving the ISMS; in the individual review of the ISMS policy; advice on monitoring threats and vulnerabilities; advice on the appropriate scope of security measures. Time spent consulting on the implementation of follow-up actions resulting from the gap analysis for the information security management system, including the provision of templates of policies and consulting on preparation for certification/assessment audits, are taken from the designated consultation hours. If required, additional consulting hours are charged at the rates set out in the Contract. Unused consulting hours expire without replacement at the end of the respective contractual year, unless a transfer of hours has been expressly agreed.
If a transfer of hours has been agreed with the option "from previous Year", unused consulting hours from the previous contractual year can be used within the first quarter of a contractual year, provided that the number of consulting hours used in the first quarter of the contractual year does not exceed half of the annual consulting hour quota. Consulting hours not used hereafter shall expire without replacement.
Insofar as a transfer of hours with the option "from previous year / next year" has been agreed, unused hours from the previous contractual year or the following contractual year can be used within a contractual year, insofar as the sum of the hours used in the contractual year does not exceed twice the annual quota of consulting hours. Consulting hours not used hereafter shall expire without replacement.

Asset Management Tool

Information assets in your organisation can be in either digital or analogue form. This includes apps, databases, cloud infrastructure, external SaaS providers, hardware, and even individual documents. The Customer can use our platform to keep track of the entire lifecycle of these information assets, classify them according to the level of protection needed, and assess associated risk for each asset. The Customer bears the responsibility for providing an up-to-date list of information assets, in the appropriate format, for upload into the DataGuard Platform, Information Security Area.

Risk Assessment Tool

The information security platform provides a Risk Assessment Tool which offers visualisation options for the risks and threats of your organisation. By using inputs from the ISMS Gap Analysis and the asset inventory, the Risk Assessment Tool will create a risk map which gives your team an overview of the Customer's risks and vulnerabilities. DataCo's information security team help the Customer to interpret these risks and define the appropriate response using the consultation hours included in the Contract. The Customer then reviews each business process, the assets involved, and reviews the associated risk.

Integrations to tools via APIs for Automation

Our DataGuard Platform offers options for API Integrations with selected tools. This will allow the Customer to import company assets into our DataGuard Platform without the need for manual data entry. The Customer must provide the relevant information and access required to set up the integration. Earliest availability of this function will be September 2022.

Corporate Identity Branded Documentation

Documentation generated by the information security platform can be branded to match the Customer's corporate identity. Documentation which may be branded with corporate identity includes infosec policies and documentation created by DataCo. Branding options are limited to adding Customer logo, adjusting font colours and adjusting fonts based on a pre-defined list. The Customer must provide all assets and information in the appropriate formats. Earliest availability of this function will be September 2022.

Enterprise Suite

The DataGuard Platform offers advanced functions for large organisations such as Single Sign-On (SSO), a corporate dashboard with overview of all entities, the capability to integrate the DataGuard platform to other software solutions and applications. These functions are in development and will be activated for the Customer upon request once released; earliest availability from April 2023. The Customer must provide any information required to facilitate set-up of these advanced functions. Integration capabilities are limited to those available within the DataGuard Integration Marketplace. DataGuard reserves the right to review Integrations usage annually and introduce additional fees for Integrations if the Customer exceeds standard usage limits.

External Chief Information Security Officer (CISO)

When commissioning this service item, the Customer will receive additional consultancy from the DataCo Information Security team, within the framework of the consulting hours included in the service and during the business hours stated above. Additional consulting hours are charged at the rates set out in the Contract. Our support services as external CISO are defined below:

- Due Diligence: Customer is supported with modifications to the ISMS due to mergers and acquisitions.
- Third party supply chain: DataGuard supports the Customer to onboard external parties securely and compliantly.
- External requests: Supporting the Customer with information security related requests from suppliers and clients.
- Regulatory bodies and authorities: Supporting the Customer with requests from regulatory bodies and authorities.
- ISMS Communication plan: Advice on how to communicate new information security policies and procedures to employees within the Customer's organisation.
- Employee audit training: Prepare employees in the Customer's organisation for the external audit by enabling them to protect your company's information.
- Introduction of new tools: Customer is advised on introducing new software and the associated processes.
- InfoSec incidents: Customer is provided support and advice on managing information security incidents.

In performing its above-mentioned support services, DataCo will not be granted any managerial powers and will assume no responsibility for the implementation of the recommended action proposed by DataCo. The Customer shall be solely responsible for this.

Support and Platform in a Secondary Language

The DataGuard Platform, Information Security Area as well as consultation from DataCo's Information Security Team is available in multiple languages. Language options are currently limited to English and German. If multilingual support is requested, the web-based information security platform can be made available in two languages; each language is accessed via a language switcher button within the platform. DataCo will ensure consultancy support is delivered in your chosen language by staffing a team to fit your requirements.

On-Site-Visits

The Customer can request an on-site visit from a DataCo Information Security Team. Exact dates and times for the on-site visit must be coordinated between both the Customer and DataCo in advance. The maximum duration of an on-site visit is eight hours. The agenda and scope of tasks to be completed during the on-site visit must be coordinated and agreed between both the Customer and DataCo in advance. Travel expenses for the on-site visit are covered by the Customer. Each on-site visit is limited to visiting a single premises.