

HiSV Data Protection Policy
Version: 2.2

Date **created**: 1 November 2025
Author: Oliver Thehos

Vithos IT-Services GbR
Martin-Schmeisser-
Weg 18
44227 Dortmund
GERMANY

Compliance & Organisation
Tel. +49 231 427888 11
E-Mail: thehos@vithos-it.de

CHANGE MANAGEMENT

Version	Date	Comment
1.0	4 August 2022	Background document on the separation of the overarching ISO 27001 standard from the GDPR (from 2017)
2.0	7 July 2024	Amendment of the policy to align it with business processes
2.1	15 July 2024	Update to the policy
2.2	1 November 2025	Update to contact details

Table of Contents

Change Management.....	2
1 Introduction.....	5
2 Objectives of the “Data Protection Policy”.....	5
3 Scope	6
4 Relation to statutory requirements	6
5 The principles governing the processing of personal data	7
5.1 Lawfulness	7
5.2 Legal framework for customer and partner data	7
5.2.1 Processing of data in the context of contractual relationships	7
5.2.2 Data processing for the purposes of advertising	8
5.2.3 Consent to the processing of personal data	8
5.2.4 Data processing on the basis of a statutory authorisation or obligation	9
5.2.5 Processing of data on the basis of a legitimate interest.....	9
5.3 Legal basis 's employee data	9
5.3.1 Data processing within the context of the employment relationship....	9
5.3.2 Data processing on the basis of legal authorisation or obligation	10
5.3.3 Collective regulations for data agreements	10
5.3.4 Consent to the processing of data	10
5.3.5 Processing of data on the basis of a legitimate interest.....	11
5.4 Data requiring special protection and their processing	11
5.5 Automated decision-making and profiling	12
5.6 Telecommunications, IT infrastructure and Internet.....	12
5.7 Information obligations and transparency	13
5.8 Purpose limitation.....	13
5.9 Data minimisation.....	13
6 Accuracy of data.....	14
6.1 Privacy by Design & Default.....	14
6.2 Restrictions on processing and erasure	14
6.3 Data security and processing procedures.....	15
6.4 Transfer of personal data	15

6.4.1	Agreement on EU Standard Contractual Clauses 2021	16
6.4.2	EU-accredited certification scheme for data transfers to the	16
6.4.3	Recognition of Binding Corporate Rules (, BCR).....	16
6.4.4	Transfer to public authorities.....	17
7	Data Protection Impact Assessment.....	17
8	Record of Processing Activities	18
9	Data processing on behalf of a controller.....	18
9.1	Requirements for the data controller	18
9.2	Requirements for contractors within the Howden Group.....	19
9.3	Requirements for other contractors	20
10	Enforceable rights for data subjects.....	21
10.1	Rights of the data.....	21
10.2	Right to lodge a complaint with the	22
11	reporting of data protection incidents.....	23
12	Data Protection Management.....	23
12.1	Responsibility of the Management Board of.....	23
12.2	Awareness-raising	23
12.3	Organisation and Data Protection Officer	24
12.4	Control measures.....	25
12.5	Disciplinary measures	25
13	Updates and amendments to the Data Protection Policy	25
14	Publication of the Data Protection Policy	25
15	Cooperation with authorities	25
16	Information on data protection on our website	26
16.1	Data protection	26
16.2	Data controller / Service provider	26
16.3	Contact details of the Data Protection Officer.....	26

1 INTRODUCTION

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG (hereinafter also referred to as HiSV) is a leading consultancy firm specialising in sports insurance in Germany and continental Europe.

HiSV was founded in the 1950s by Erwin Himmelseher as a family business. Customers particularly value the quality of the work, the personal, trusting relationship with their points of contact, and the rigorous decision-making processes.

Our clients' trust in our exceptional service is HiSV's greatest asset, and all the data protection processes and measures set out in this policy, as well as our additional commitment to implementing ISO 27001 (the international standard for information security), serve the aim of protecting HiSV's values and the personal data entrusted to us by our clients and partners.

2 OBJECTIVES OF THE "DATA PROTECTION POLICY"

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG regards the protection of the personal rights of its employees, customers and partners as an essential part of its social and corporate responsibility.

Like many other countries, the European Union has enacted legal standards for the protection of personal data (the EU GDPR). Together with the supplementary German Data Protection Act (BDSG) and other binding standards, these give rise to processes and measures for the protection of data-relevant information.

This includes, for example, the requirement that data may only be transferred to other countries if an adequate level of data protection is guaranteed by the recipient, or that personal data may only be collected or processed under certain conditions.

This Data Protection Policy defines a uniform and high standard of protection for the processing of data subject to data protection regulations within the European Economic Area (hereinafter referred to as the 'EU/EEA'), as well as for the collection, processing and transfer of personal data to group companies and partners outside the EU/EEA (including its subsequent processing there). This privacy policy takes particular account of the provisions of the Swiss Data Protection Act (DSG), the EU GDPR and the UK GDPR. The actual applicability of the aforementioned laws is assessed on a case-by-case basis and implemented accordingly.

The implementation of this policy provides appropriate safeguards regarding the data and information entrusted to HiSV to ensure compliance with the legal principles set out in Article 5 of the GDPR

- Lawfulness of processing in good faith
- Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity
- Confidentiality
- Accountability

3 SCOPE

This Data Protection Policy applies to HiSV, its branches and all employees and members of the executive bodies.

This policy applies to the processing of personal data in filing and storage systems (including in paper form). As a rule, no distinction is made between automated and non-automated processing.

The policy applies to the processing of personal data by HiSV and its branches located within the EU/EEA or in any other country to which this policy may be extended.

This policy may be extended to countries outside the EU/EEA. In countries where data relating to legal entities is protected in the same way as personal data, this policy also applies to data relating to legal entities in the same manner.

The provisions of this policy are binding on Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG and its branches, provided that they operate within the scope of application.

In addition to the applicable regulations of the European Union and national data protection laws, responsibility for compliance with this policy therefore lies with the management and staff of HiSV.

Branches may not adopt any deviating regulations, provided that there are no conflicting legal requirements and that such exceptions have been approved in writing by the Data Protection Officer and the management of Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG.

4 RELATION TO STATUTORY REQUIREMENTS

This Data Protection Policy does not replace applicable law. Where national data protection laws or the EU GDPR stipulate a higher level of protection for personal data, those provisions take precedence over this Policy.

The policy shall also be applied where no corresponding legislation exists at national level (third countries). The approach to the application of the data protection policy in third countries is described in Section 16.

In the event of a breach of national law resulting from compliance with this policy, or where it is necessary to introduce provisions that diverge from this policy, this must be reported to the Data Protection Officer.

Should conflicts arise between national legislation and this Policy, it is the responsibility of the Data Protection Officer and the management of HiSV, in consultation with the relevant branch, to devise a practical solution that is consistent with the objective of this Policy.

5 THE PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

All obligations listed in Section 5 confer third-party beneficiary rights on the data subject .

5.1 Lawfulness

The processing of personal data is only permissible if it is carried out lawfully and in good faith. Data processing must therefore be based on an appropriate legal basis that permits the respective processing operation.

This provision also applies to data processing between HiSV's branches or HiSV's sister companies within the Howden Germany Group.

However, the fact that both the transferring and the receiving company belong to the Howden Deutschland Group or a branch of HiSV does not in itself constitute grounds for data processing.

The processing of personal data is permitted, inter alia, in accordance with clauses 5.2 or 5.3, provided that one of the grounds for authorisation specified therein applies. This also applies in the event that the purpose of processing personal data is to be changed from the original intended purpose.

5.2 Legal framework for customer and partner data

5.2.1 Processing of data in the context of contractual relationships

The processing of a data subject's personal data – for example, that of a prospective customer, customer or partner – is permitted where this is necessary for the conclusion, performance and termination of a contract.

This also includes, insofar as it relates to the purpose of the contract, the provision of customer or partner support.

The processing of personal data prior to the conclusion of a contract is permitted, provided that it serves the purpose of preparing quotations, initiating the contract or fulfilling other enquiries from the prospective customer aimed at concluding a contract.

During the pre-contractual phase, the prospective customer may be contacted using the data they have themselves provided. Any restrictions expressed by the prospective customer must be taken into account.

5.2.2 Data processing for the purposes of advertising

Where the data subject contacts HiSV with a request for information, for example requesting that information material be sent to them, data processing is permitted for the purpose of fulfilling this request.

Measures intended to retain customers or promote products are subject to further legal requirements. The processing of personal data for the purposes of advertising or market and opinion research is permitted, provided this is compatible with the purpose for which the data was originally collected. The data subject must be informed in advance of the use of their data for advertising purposes.

If data is collected exclusively for advertising purposes, the data subject must be informed that the provision of data for these purposes is voluntary. Consent must be obtained from the data subject as part of the communication process.

With regard to consent, the data subject has the option to choose between different contact channels, including electronic communication and telephone calls (see Consent, Section 5.2.3).

If the data subject objects to the use of their data for marketing purposes, any further use of their data for such purposes is prohibited. In this case, the data in question must be restricted or blocked for marketing purposes.

Furthermore, the restrictions arising from national legislation on the use of data for marketing purposes must be observed.

5.2.3 Consent to the processing of personal data

Data processing may take place on the basis of the data subject's consent. Before consent is given, the data subject must be informed in accordance with this Data Protection Policy.

For evidential purposes, the declaration of consent must generally be obtained in writing or electronically. In exceptional cases, such as during a telephone consultation, consent may also be given verbally. The granting of consent must be documented.

5.2.4 Data processing on the basis of a statutory authorisation or obligation

Provided that national legislation requires, stipulates or permits the processing of personal data, such processing is also lawful.

The nature and scope of data processing must be guided by and comply with the criteria required for legally permissible data processing.

5.2.5 Processing of data on the basis of a legitimate interest

Personal data may also be processed where this is necessary to pursue a legitimate interest.

Legitimate interests can generally be classified into two categories. On the one hand, they may be of a legal nature, for example in the context of enforcing outstanding claims. On the other hand, they may be of an economic nature, for example in the context of preventing contractual disruptions.

The processing of personal data on the basis of a legitimate interest is not permitted if, in the specific case, the data subject's interests in the protection of their data outweigh the legitimate interests in the processing.

An assessment of the interests' worthy of protection is required in the context of any processing.

5.3 Legal basis 's employee data

5.3.1 Data processing within the context of the employment relationship

The processing of personal data necessary for the establishment, performance and termination of the employment relationship is permitted within the context of the employment relationship.

In the context of decision-making regarding the establishment of an employment relationship, the processing of applicants' personal data is permitted.

In the event of a rejection, the applicant's data must be deleted, taking into account the time limits for the preservation of evidence, unless the applicant has consented to further storage for a subsequent selection process.

Consent is also required if the data is to be used for further recruitment processes or before the application is passed on to other members of the Howden Germany Group.

Within the context of an existing employment relationship, the processing of data must always be limited to the purpose of the employment relationship, unless one of the grounds for data processing set out below applies.

If, during the process of establishing an employment relationship or whilst an employment relationship is in force, it is necessary to collect further information

about the applicant from a third party, the relevant national legal requirements must be taken into account. In case of doubt, the data subject's consent must be obtained.

The processing of personal data that relates to the employment relationship but does not primarily serve the purpose of establishing or terminating the employment relationship (employee data) is only permitted if one of the following legal bases applies.

5.3.2 Data processing on the basis of legal authorisation or obligation

The processing of employee data is also permitted provided that national legislation requires, stipulates or permits such data processing.

The nature and scope of data processing must be in accordance with the statutory grounds for authorisation and must be necessary for the data processing permitted by law.

Where there is a legal margin for discretion, the employee's legitimate interests must be taken into account.

5.3.3 Collective regulations for data agreements

Processing that goes beyond the purpose of fulfilling the contract is also permissible if it is authorised by a collective agreement.

Collective agreements are understood to mean collective bargaining agreements as well as agreements between employers and employee representatives, which are concluded within the framework of the respective labour law.

The relevant provisions must relate to the specific purpose of the intended processing and may be formulated within the framework of national data protection law.

The relevant provisions must cover the specific purpose of the intended processing. It should be borne in mind that they may be structured within the framework of EU regulations and national laws.

5.3.4 Consent to the processing of data

The processing of employee data may take place on the basis of a declaration of consent given voluntarily. It must be ensured that the declaration is not given under pressure and that the data subject has been adequately informed of their rights prior to giving consent. Failure to give consent must not result in any disadvantage for employees. Consent that is not given voluntarily is invalid.

For evidential purposes, the declaration of consent is generally recorded in writing or stored electronically. Where, in exceptional circumstances, this is not possible, consent may be given verbally. The giving of verbal consent, as well as the provision of adequate information – including this data protection policy – must be duly documented in all cases.

5.3.5 Processing of data on the basis of a legitimate interest

The processing of employees' personal data may also take place where this is necessary to pursue a legitimate interest on the part of HiSV. Legitimate interests are generally based on legal grounds (e.g. the assertion, exercise or defence of legal claims) or economic grounds (e.g. streamlining operational processes, company valuation).

The processing of personal data on the basis of a legitimate interest is not permitted if, in a specific case, there are indications that the employee's interests worthy of protection outweigh the interest in the processing. In the context of any processing, an assessment must be carried out to determine whether the employee's interests worthy of protection are affected.

The processing of employee data that goes beyond the performance of the employment relationship – for example, in the context of performance monitoring – is only permissible if there is a legal obligation or a legitimate reason for doing so. Even where a legitimate reason exists, the proportionality of the monitoring measure must be subject to critical scrutiny.

HiSV is, in principle, permitted to carry out a monitoring measure, provided that the objectives pursued by it are deemed legitimate. These include, for example, compliance with legal provisions and internal company rules. However, when weighing up the interests involved, the legitimate interests of the employee affected by the measure must also be taken into account. A monitoring measure may therefore only be carried out if it is proportionate in this specific case.

As part of the decision-making process, the existence of a legitimate interest on the part of the group company, as well as the existence of any interests of the employees that may be worthy of protection, must be determined and documented.

Furthermore, where applicable, any additional requirements arising from applicable national law must be taken into account. These include, for example, the co-determination rights of employee representatives and the information rights of the data subjects.

5.4 Data requiring special protection and their processing

The processing of personal data classified as requiring special protection is only permitted under certain conditions. Data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life is considered to require special protection.

Furthermore, data relating to criminal offences is often subject to specific processing conditions imposed by national law.

The processing of data requiring special protection due to its sensitivity is only permitted if there is a legal basis for doing so. This means that the processing is

either required or permitted by law, for example to assert, exercise or defend legal claims against the data subject, or to comply with rights and obligations under employment or social security law.

Furthermore, the processing of data is permitted provided that the data subject has voluntarily and expressly consented to the processing. This may be the case, for example, when data is processed to draw up a quotation, during pre-contractual negotiations or for the performance of a contract.

The Data Protection Officer must be informed in advance if the processing of personal data requiring special protection is planned.

5.5 Automated decision-making and profiling

A decision based solely on automated processing which has legal or similarly adverse effects on the data subject is permissible only if it is necessary for the conclusion or performance of a contract, or if the data subject has given their explicit consent. In individual cases, an automated decision may involve profiling, whereby the processing of personal data is used to assess individual personality traits (for example, the creditworthiness of customers and business partners, or the creation or evaluation of skills profiles in the context of recruitment).

Where personal data is processed automatically in the context of an employment relationship, it must be ensured that the automated processing or the conclusions drawn from it do not form the sole basis for decisions with negative consequences or significant adverse effects on the employees concerned.

In general, the data subject must be informed of both the fact and the outcome of an automated individual decision. Furthermore, they must be given the opportunity to have the decision reviewed on a case-by-case basis by a data controller.

5.6 Telecommunications, IT infrastructure and Internet

Computers, smartphones, telephone systems, email addresses, the intranet and the internet, etc., as well as internal social networks, are primarily provided by the company to enable the performance of work-related tasks. These constitute work equipment and company resources, the use of which is permitted within the framework of the applicable legal provisions and the company's internal guidelines.

General monitoring of telephone and email communications, as well as intranet and internet usage, takes place. To defend against attacks on the IT infrastructure or on individual users, protective measures have been implemented, including at the network access points. The purpose of these protective measures is to block technically harmful content and to analyse potential attack patterns.

The use of telephone systems, email addresses, the intranet and the internet, as well as internal social networks, is logged for reasons of security and traceability.

The analysis of personal data is only permitted in the event of a specific, well-founded suspicion of a breach of laws or company policies. In doing so, the principle of proportionality must be upheld. It must be borne in mind that national legislation applies. The analyses are not used for performance monitoring and are carried out by several people only after consultation with the Data Protection Officer and the management.

5.7 Information obligations and transparency

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG is obliged to inform data subjects of the purposes and circumstances of the processing of their personal data in accordance with Articles 13 and 14 of the GDPR. The information must be provided in a precise, transparent, comprehensible and easily accessible form, using clear and plain language.

It must be ensured that data protection requirements are observed at all times. This information must therefore, as a general rule, be provided at the time of the initial collection of personal data.

The information must, as a general rule, be provided at the time of the initial collection of personal data. In the event that HiSV transfers personal data to a third party, the information must be communicated to the data subjects within a reasonable period after the third party has received the data.

If the data subject already possesses the relevant information, if providing this information proves impossible, or if the effort required to provide notification would be disproportionate, there is no further obligation to provide information. Should any of these exceptions apply, this must be documented in writing or electronically.

5.8 Purpose limitation

The processing of personal data is only permitted if it is carried out for the purpose defined prior to the collection of the data. A subsequent change to the purpose of processing is only permitted provided that the processing is compatible with the purposes for which the personal data was originally collected.

5.9 Data minimisation

The processing of personal data must be carried out in a manner that ensures both quantitative and qualitative restrictions. These restrictions are intended to ensure that the data is processed only to the extent necessary to achieve the specified purposes.

This aspect must be taken into account right from the design stage of data collection. Where the purpose permits and the effort involved is proportionate to the objective pursued, the use of anonymised or statistical data should be considered.

6 ACCURACY OF DATA

The personal data held must be factually accurate and up to date. HiSV is obliged to take appropriate measures to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

6.1 Privacy by Design & Default

The 'Privacy by Design' principle requires HiSV to establish state-of-the-art internal strategies and take all necessary measures to incorporate or integrate data protection principles from the outset into the specification and architecture of business models and processes, as well as IT systems used for data processing. This is carried out with due regard to the data protection principles, which have already been taken into account as fundamental elements during the conception and design phase.

The 'Privacy by Design' principle states that the procedures and systems for processing personal data must be designed in such a way that their initial settings are limited to the data processing necessary to fulfil the purpose (the 'Privacy by Default' principle). This encompasses the scope of processing, the retention period and accessibility.

Further measures may include the pseudonymisation or anonymisation of personal data as soon as practicable, ensuring transparency regarding the functions and processing of personal data, guaranteeing the data subject's freedom of choice regarding the processing of their personal data, and enabling the development and continuous improvement of security features by the operator of the procedures or systems.

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG implements appropriate technical and organisational measures throughout the entire lifecycle of its processing operations to ensure compliance with the aforementioned principles. These measures are maintained and documented throughout the entire lifecycle.

6.2 Restrictions on processing and erasure

The storage and processing of personal data is permitted only for as long as is necessary for the specific purpose for which it is being processed. This means that the data must be deleted as soon as the purpose of its processing has been fulfilled or the necessary grounds for processing have otherwise ceased to apply.

Where statutory retention obligations apply and the data must continue to be stored, the processing must be restricted or the data anonymised.

Those responsible for the individual processes must ensure that the deletion and anonymisation procedures are implemented for their processes and, where necessary, documented in writing or electronically.

6.3 Data security and processing procedures

It must be ensured that personal data, regardless of whether data processing is carried out electronically or on paper, is protected against unauthorised access, unlawful processing or disclosure, as well as against accidental loss, alteration or destruction.

Before introducing new data processing procedures, in particular new IT systems and associated processes, technical and organisational measures for the protection of personal data must be defined and implemented. These measures must be based on the current state of the art, the risks associated with the processing and the data's protection requirements.

As part of the data protection impact assessment and the record of processing activities, the data controllers must document the technical and organisational measures relevant to data protection.

The technical and organisational measures for the protection of personal data form an integral part of the company-wide information security and data protection management system.

Continuous adaptation to technical developments, organisational changes and legislative updates, as well as taking into account the threat landscape for IT infrastructures and data processing, is essential.

To ensure compliance with these requirements, HiSV collaborates with internal and external experts working across disciplines. The measures and processes implemented are continuously refined through joint efforts.

6.4 Transfer of personal data

The transfer of personal data to recipients outside HiSV or to recipients within the Howden Group is subject to the conditions for the lawfulness of processing personal data set out in Section 5. The recipient of the data must be obliged to use it only for specified purposes.

In the event of a cross-border transfer of personal data (including the granting of access from another country), the relevant national requirements for the transfer of personal data abroad must be met.

Data transfers within the EEA do not require authorisation, as the level of protection for data transfers in these countries is uniformly regulated.

However, the processing of personal data from the EU/EEA in a third country outside the organisation is only permitted if the recipient can demonstrate that it has a data protection standard that complies with this policy. Suitable instruments include:

6.4.1 Agreement on EU Standard Contractual Clauses 2021

In the event of the transfer of personal data to non-European third countries, HiSV must demonstrate an appropriate legal basis in accordance with the General Data Protection Regulation (GDPR) for the data transfer. In addition, it must be ensured that the recipient of the data guarantees an adequate level of protection.

The EU Standard Contractual Clauses are model contracts drawn up by the European Commission which oblige both contracting parties to comply with a level of data protection comparable to that of the EU.

The European Commission assesses whether an adequate level of protection is guaranteed in third countries outside Europe. If an adequate level of data protection is guaranteed, the Commission issues an adequacy decision.

The exemption from authorisation when using the standard contractual clauses applies only if they are used without modification. However, this provision does not apply to the selection of a module or the addition or updating of information in the annex.

Furthermore, the contracting parties have the option of incorporating the standard contractual clauses into a more comprehensive contract. However, if further clauses or additional safeguards are included in the contract, these must not conflict, either directly or indirectly, with the standard contractual clauses, nor must they infringe upon the fundamental rights or freedoms of the data subjects.

6.4.2 EU-accredited certification scheme for data transfers to the

Certification is an instrument under the GDPR (Articles 42 and 43) designed to provide reliable evidence of compliance with data protection provisions. An approved certification mechanism, through its legally binding and enforceable obligations to comply with the safeguards, including the rights of data subjects (Art. 46(2)(f), 42(2) GDPR), can serve as an adequate guarantee that sufficient protection for personal data is ensured when data is transferred to a third country.

6.4.3 Recognition of Binding Corporate Rules (, BCR)

The transfer of data to third countries without an adequate level of data protection may take place on the basis of binding internal data protection rules, known as Binding Corporate Rules (BCR), provided that data subjects have enforceable rights and effective legal remedies at their disposal. Furthermore, the BCR must have been approved by a competent supervisory authority. Consequently, specific transfers to which the BCR apply are not subject to separate authorisation.

BCRs apply to groups of companies or groups of undertakings carrying out a joint economic activity. According to Article 4(19) of the GDPR, a group of companies is a group consisting of a controlling undertaking and its subsidiaries. The minimum requirements for BCRs are set out in Article 47 of the GDPR.

BCRs can be used in two forms:

Rules for controllers: Controller BCRs (BCR-C)

These rules apply to data that data controllers in EU countries send to other data controllers or data processors outside the EU. In this context, the companies involved all belong to the same group.

This instrument is suitable for corporate groups or groups of companies where large volumes of data are exchanged. The companies draw up data protection rules for all individuals whose data is processed within the group. These rules may also be limited to specific areas, such as the processing of personnel data.

Regulations for data processors: Processor BCR (BCR-P)

These rules apply to data processors. They relate to data received from a data controller who is not a member of the group and which is subsequently processed by members of the group acting as data processors and/or sub-processors. This may occur, for example, when IT services are outsourced. These provisions may also be referred to as 'BCRs for third-party data'.

6.4.4 Transfer to public authorities

The transfer of personal data to a public authority is only permitted, provided that it is not carried out on a mass scale, disproportionately or indiscriminately. In the event of conflicts between these requirements and official regulations, the Data Protection Officer must, in collaboration with senior management, find a workable solution that is consistent with the purpose of this policy.

7 DATA PROTECTION IMPACT ASSESSMENT

When introducing new processing operations, or in the event of a significant change to existing, previously assessed processing operations, HiSV or the Data Protection Officer shall carry out a prior analysis to determine whether the processing poses a significant risk to the privacy of data subjects.

This applies in particular in the context of the use of new technologies. In this context, particular consideration must be given to the nature, scope, context and purpose of the data processing.

As part of this risk analysis, the Data Protection Officer carries out an assessment of the impact of the planned processing operations on the protection of personal data (data protection impact assessment). If, following the data protection impact assessment and despite the implementation of appropriate risk mitigation measures, there remains a high risk to the rights and freedoms of data subjects, but the processing operation is essential for HiSV, the Data Protection Officer shall, after consultation with the management, consult the competent data protection supervisory authority.

8 RECORD OF PROCESSING ACTIVITIES

HiSV is obliged to document the procedures in which personal data is processed in a record of processing activities. This record must be available and maintained in written or electronic form. It must be made available to the competent data protection supervisory authority upon request.

9 DATA PROCESSING ON BEHALF OF A CONTROLLER

The term 'data processing on behalf of a client' refers to the processing of personal data by a service provider on behalf of and in accordance with the instructions of the client. In this context, a written agreement on data processing on behalf of a client must be concluded between the service provider and the client, which complies with the applicable legal requirements. The client retains full responsibility for the correct execution of the data processing.

The provisions of clause 8.2 also apply to contractors who are members of the Howden Germany Group.

9.1 Requirements for the data controller

When commissioning the processing of personal data, the following requirements must be taken into account, whereby HiSV, as the data controller, must ensure compliance with the following requirements.

When selecting a data processor, care must be taken to ensure that the data processor possesses the necessary competence to meet the requirements for technical and organisational safeguards.

In addition, the standard contract clauses provided by the Data Protection Officer must be taken into account.

The instruction to process data by external service providers must be issued in writing or in electronic form. Furthermore, the client's instructions regarding data processing, as well as the responsibilities of the client and the contractor, must be documented.

Before data processing commences, it is the client's responsibility to take appropriate measures to ensure that the contractor fulfils the obligations set out in this context. A contractor may demonstrate compliance with data protection requirements, in particular, by means of appropriate certification of an adequate information security system. Depending on the risk associated with the data processing, such audits must be repeated regularly during the term of the contract and the results must be documented.

9.2 Requirements for contractors within the Howden Group

Contractors within the Howden Group may also process personal data only in accordance with the GDPR and in accordance with instructions from HiSV.

The engagement of other sister or group companies or third parties, also referred to as sub-contractors, for the purpose of processing personal data on the contractor's own behalf or on its behalf as a sub-contractor requires prior review and approval by Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG.

Consent shall be granted solely on condition that the contractor obliges the sub-contractor, either contractually or in a similarly legally binding manner, to fulfil the same data protection obligations that the contractor is subject to under this policy vis-à-vis HiSV and the data subjects. Furthermore, the contractor must guarantee that appropriate technical and organisational safeguards are in place.

The terms of the consent, as well as the information obligations in the event of changes to the subcontracting relationship, must be set out in the service contract.

Contractors are obliged to provide HiSV, as the client, with appropriate support in complying with the data protection provisions applicable to it. This includes, in particular, the provision of all information necessary to demonstrate such compliance. This applies in particular to compliance with the following aspects:

The general principles governing processing (see clause 5), the rights of data subjects (see clause 10), the data controller's reporting obligations (see clause 12), the provisions applicable to data controllers and data processors (see clause 8), and the handling of enquiries and investigations by supervisory authorities must also be taken into account.

Where applicable standards or legal provisions require the data processor to process data in a manner contrary to these instructions, or prevent the data processor from fulfilling its obligations under this policy or the data processing agreement, the data processor is obliged to notify HiSV of this without delay, unless the relevant legal provision prohibits such notification.

This provision also applies where the data processor is unable, for other reasons, to comply with the instructions of the data controller. In such a case, the data controller is entitled to suspend the transfer of data and/or terminate the data processing agreement.

Every contractor is obliged to inform the client of any legally binding request from a public authority for the disclosure of personal data, unless this is prohibited for other reasons.

Upon completion of the provision of services, the contractor must either delete or return all personal data provided by the client. The choice as to which of these two options the contractor must fulfil rests with the client.

Contractors are obliged to inform their client immediately of any claims, demands or complaints made by data subjects.

Clients within the group are also obliged to ensure that external contractors comply with the above provisions.

The contractor's specific obligations towards the client have a third-party beneficiary effect.

9.3 Requirements for other contractors

The processing of personal data by the contractor must be carried out exclusively in accordance with the instructions of HiSV as the client.

The engagement of third parties, known as sub-contractors, by the contractor to process personal data on the contractor's own behalf is only permitted with the prior consent of the client.

Consent to engage a third party may be granted only if the Contractor contractually or otherwise legally binds the sub-contractor to the same data protection obligations that apply to the Contractor under this policy in relation to HiSV and the data subjects. The Contractor must also ensure that appropriate technical and organisational safeguards are in place.

The terms of such consent, as well as the information obligations in the event of changes to the sub-contracting relationship, must be set out in the service contract.

Contractors are obliged to provide HiSV, as the client, with appropriate support in complying with the data protection provisions applicable to it. This includes, in particular, the provision of all information necessary to demonstrate such compliance.

The general principles governing processing (see clause 5), the rights of data subjects (see clause 10), the client's reporting obligations (see clause 12), the provisions for clients and contractors (see clause 8), and the handling of enquiries and investigations by supervisory authorities must also be taken into account.

Where applicable standards or legal provisions require the Contractor to process data in a manner contrary to these instructions or prevent the Contractor from fulfilling its obligations under this Policy or the Data Processing Agreement, the Contractor is obliged to notify HiSV of this without delay, unless the relevant legal provision prohibits such notification.

Each Contractor is obliged to inform the Client of any legally binding request from a public authority for the disclosure of personal data, unless this is prohibited for other reasons.

Upon completion of the provision of services, the data processor must either delete or return all personal data provided by the data controller. The choice as to

which of these two options the data processor must fulfil rests with the data controller.

Contractors are obliged to inform their client immediately of any claims, demands or complaints made by data subjects.

The Contractor's specific obligations towards the Client are for the benefit of the data subject as a third party.

10 ENFORCEABLE RIGHTS FOR DATA SUBJECTS

All rights of data subjects listed in Clause 9, as well as HiSV's obligations, are structured to confer third-party beneficiary rights on the data subject.

Enquiries and complaints submitted in accordance with this Section 9 must be examined within one month and, where necessary, responded to. Taking into account the complexity and the number of requests, this one-month period may be extended by a maximum of two further months. The data subject must be informed of this extension accordingly.

10.1 Rights of the data

A data subject in the EU/EEA has the following rights vis-à-vis HiSV or – where HiSV is acting as a data processor – vis-à-vis the data controller, as set out in detail in EU law:

- The right to information regarding the circumstances of the processing of personal data must be guaranteed. In this regard, the guidelines of the EU Data Protection Supervisor must be taken into account.
- Exercising the right of access includes the possibility of obtaining information about the manner in which personal data is processed and about the rights to which the data subject is entitled. Where specific rights of access to the employer's records are provided for in the relevant labour law provisions – for example, the personnel file – these remain unaffected. If the data subject so wishes, a copy of the personal data may be provided in return for a reasonable fee. However, this does not apply if it would prejudice the legitimate interests of third parties.
- The data subject has the right to have their personal data rectified or supplemented if it is inaccurate or incomplete.
- The data subject may exercise the right to restrict the processing of personal data if they contest the accuracy of the data, if the company no longer requires the data for processing, or if the data subject still requires the data to exercise their legal claims. Furthermore, the data subject has the right to request that the company restrict the processing of their data. This is particularly the case where the company would otherwise be required to erase the data or is assessing an objection raised by the data subject.

- The right to erasure of the data applies where consent is withdrawn or the legal basis for processing the data no longer exists. The data must also be erased if the purpose of the data processing no longer applies due to the expiry of time limits (e.g. retention periods) or for other reasons. Erasure is not permitted where there is an existing retention obligation or where there are conflicting legitimate interests.
- the right to receive the personal data concerning them and provided by them, which has been lawfully processed, in a commonly used digital format and to transmit this to a third party, provided that the processing is carried out by automated means and is technically feasible.
- The right to object to marketing and advertising activities at any time must be guaranteed. To this end, an appropriate consent and objection process must be established. For these purposes, this data must be blocked.
- A general right to object to the processing of personal data must be taken into account where the data subject's legitimate grounds – such as their interests, rights and freedoms – override HiSV's legitimate interest in the processing. However, this right does not apply where a legal provision requires the processing of the data. In the event of a valid objection, the data in question must be deleted within the prescribed time limit.

Furthermore, the data subject has the right to assert their rights against the sister company within the Howden Group in a third country that imports the data.

10.2 Right to lodge a complaint with the

In accordance with the EU General Data Protection Regulation (GDPR), data subjects are entitled to lodge a complaint with HiSV's Data Protection Officer if they believe that this policy has been breached. The complaint may be submitted by email to hisv@vithos-dsgvo.de or by telephone (on working days between 09.00 and 16.30) on +49 231 42788811.

If the complaint is justified, Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG will take appropriate measures to ensure compliance with this policy and will inform the data subject of the measures taken and their further rights.

Should the data subject not accept HiSV's decision regarding compliance with the regulations (or should there be dissatisfaction with the handling of the matter for other reasons), it is possible to take legal action against this decision or conduct.

In this context, it is possible to contact the competent supervisory authority, whereby, in particular, the data subject's habitual residence, place of work or the location of the alleged infringement shall serve to determine jurisdiction. Another option is to bring legal proceedings before a court. Further statutory rights and responsibilities remain unaffected by this.

11 REPORTING OF DATA PROTECTION INCIDENTS

In the event of a potential breach of data security requirements – hereinafter referred to as a ‘data protection incident’ – the company is subject to obligations to investigate, provide information and mitigate damage. A data protection incident is defined as a data breach where there is a breach of data security that directly results in the erasure, alteration, unauthorised disclosure or use of personal data.

Should this give rise to a risk to the rights and freedoms of natural persons, such incidents must be reported to the competent supervisory authority within 72 hours of the company becoming aware of the breach.

Furthermore, in the event of a data breach that is likely to result in a high risk to the personal rights and freedoms of data subjects, the data subjects must be notified of the data breach.

Contractors within the meaning of clauses 8.2 and 8.3 are obliged to report data protection incidents to their client without delay.

In the event of a data breach, appropriate documentation must be drawn up and made available to the supervisory authority upon request.

12 DATA PROTECTION MANAGEMENT

12.1 Responsibility of the Management Board of

The management is responsible for data processing within its area of responsibility. It is obliged to ensure that statutory data protection requirements (e.g. national reporting obligations) and those set out in this Data Protection Policy are observed.

The management’s responsibility includes ensuring that data is processed properly in accordance with data protection requirements through organisational, personnel and technical measures.

The implementation of the specified guidelines is the responsibility of the relevant staff members. In the event of data protection inspections by the authorities, the Data Protection Officer and the management must be informed immediately.

12.2 Awareness-raising

Management must ensure that HiSV employees who have permanent or regular access to personal data, or who are involved in the collection of data or the development of tools for processing personal data, understand and comply with this policy. In addition to this policy, guidelines and regular training on data protection and information security also serve to achieve the aforementioned objectives.

12.3 Organisation and Data Protection Officer

In their role as Data Protection Officer, the Data Protection Officer is independent of instructions regarding the performance of their duties. As a body that is functionally independent of instructions, the Data Protection Officer works to ensure compliance with data protection regulations. They are responsible for ensuring that national and international data protection regulations are complied with. This also includes monitoring compliance with and updating this policy.

The Data Protection Officer is authorised to:

- to work towards ensuring that data protection regulations are observed and complied with
- to inspect and assess office premises from a data protection perspective
- to seek feedback from within the departments
- to instruct staff on data protection compliance
- to report any grossly negligent breaches of data protection regulations to the management without delay

The Data Protection Officer shall promptly inform the management of any data protection risks and shall be available to provide advice on finding solutions.

Any data subject may contact the Data Protection Officer with suggestions, enquiries, requests for information or complaints relating to data protection or data security.

The Data Protection Officer is therefore available to all data subjects at any time to discuss concerns, questions, requests for information or complaints relating to data protection or data security. Upon request, concerns and complaints will be treated confidentially.

The contact details of the Data Protection Officer are as follows:

Vithos IT-Services GbR
-Büro Dortmund-
Oliver Thehos
Martin-Schmeisser-Weg 18
44227 Dortmund
Germany

Telephone number: +49 231 427888 18

E-mail: hisv@vithos-dsgvo.de

12.4 Control measures

Compliance with this policy and the applicable data protection laws is continuously monitored within the company by means of a risk-based review. Responsibility for this lies with the Data Protection Officer.

12.5 Disciplinary measures

The processing of personal data is regulated by relevant legislation in many countries, and failure to comply with these laws may result in legal consequences. These include both administrative penalties and civil claims for damages.

Responsibility for compliance with this policy lies with every individual employee of HiSV. Breaches of the data protection policy caused by employees may result in sanctions under employment law. Breaches are dealt with in accordance with internal regulations.

13 UPDATES AND AMENDMENTS TO THE DATA PROTECTION POLICY

This policy may be amended at any time in consultation with the Data Protection Officer. Should any changes be made that have a significant impact on the data protection policy or that may compromise the level of protection afforded, the management must be informed immediately.

14 PUBLICATION OF THE DATA PROTECTION POLICY

It is of essential importance to HiSV that data subjects have easy access to this policy. For this reason, the latest version of this policy is available on the HiSV website.

This provision is in the interests of data subjects as third-party beneficiaries.

15 COOPERATION WITH AUTHORITIES

In the event of problems, enquiries or other proceedings arising from the processing of personal data, both within the EU/EEA and in third countries, HiSV is obliged to cooperate with the competent supervisory authorities.

This obliges HiSV to accept audits carried out by the competent supervisory authorities in accordance with the law and to comply with instructions from the supervisory authorities arising from the application of the GDPR in the case of processing operations within the EU/EEA as well as in third countries, or arising from the provisions of this policy.

The provisions of clause 14 regarding cooperation with the authorities are designed to confer third-party beneficiary rights.

16 INFORMATION ON DATA PROTECTION ON OUR WEBSITE

16.1 Data protection

On the HiSV website, HiSV provides you with detailed information about which personal data (hereinafter referred to as 'data') is collected and processed when you visit our website. We also explain what kind of data we collect, process and protect from our customers.

When using specific terms such as 'controller' or 'processing' etc., we refer to the definitions in the GDPR (e.g. Article 4).

16.2 Data controller / Service provider

The data controller within the meaning of the Federal Data Protection Act (BDSG) and, at the same time, the service provider within the meaning of the Digital Services Act (DDG) is Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG; please refer to the legal notice for further details.

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG
Theodor-Heuss-Ring 23
50668 Cologne
Germany

Telephone number: +49 (0)221 888 25 – 100
E-Mail: hisv@himmelseher.com

16.3 Contact details of the Data Protection Officer

Vithos IT-Services GbR
-Büro Dortmund-
Oliver Thehos
Martin-Schmeisser-Weg 18
44227 Dortmund
Germany

Telephone number: +49 231 427888 18
E-mail: hisv@vithos-dsgvo.de