STANDARD DATA PROCESSING AGREEMENT

Lucas IT B.V.

Consisting of:

Deel 1. Data Pro Statement

Part 2. Standard clauses for processing

Edition December 2025

Version 1.4

DEEL 1: DATA PRO STATEMENT

This Data Pro Statement, together with the Standard Clauses for Processing, forms the processing agreement for the service of the company that has drawn up this Data Pro Statement.

GENERAL INFORMATION

1. This Data Pro Statement has been prepared by:

Lucas IT B.V. has its registered office and principal place of business at Philippus Robbenstraat 9A, 7665 AA Albergen, Chamber of Commerce: 06091413.
For questions about this Data Pro Statement or data protection, please contact:
privacy@lucasit.nl and/or 0546-442322

2. This Data Pro Statement applies from and concerns version 22-5-2018 1.4

We regularly adjust the security measures described in this Data Pro Statement in order to remain prepared and up-to-date with regard to data protection. We will keep you informed of new versions through our normal channels.

3. This Data Pro Statement applies to the following services of the processor

A. **Proactive Monitoring**
B. **Support**
C. **Management & Maintenance**
D. **Antivirus**
E. **Firewall**
F. **Anti-spam & ATP**
G. **Email**
H. **Cloud storage**
I. **Hosted werkplek**
J. **Microsoft 365 Copilot & Azure**
K. **Google Apps**
L. **Web Hosting**
M. **VoIP**
N. **Backup**
O. **Colocation**
P. **Internet services**
Q. **Hosted Bureaublad**
R. **VPS**
S. **MDR**
T. **Security Awareness**
U. **Centrale Management Systems**
V. **Dark Web Monitoring**
W. **MFA**
X. **SaaS Monitoring**
Y. **Automated Pentest**
Z. **Professional Service Automation tool**
AA. **Newsletter system**
BB. **Central signature software**
CC. **Internet services**
DD. **Credentials Management System**
EE. **Password vault**
FF. **Managed Wi-Fi controller**

4. Description of services

A. Monitoring

24x7 Monitoring of the system processes and control of the IT environment through digital heart monitoring.

B. Support

Remote and on-site support for the IT environment.

C. Management & Maintenance

Maintenance and management of the IT environment and IT components.

D. Antivirus

: Protection, IT environment, IT components, on-premise or cloud antivirus.

E. Firewall

Gatekeeper of network to monitor and secure incoming and outgoing traffic.

F. Anti-spam & ATP

Cloud services to clean up and secure mail and/or surfing traffic.

G. Email

Email Server from the Cloud, for mail, calendar, address book and tasks.

H. Cloud storage

Cloud service for storage files, such as text files, photo files, video files, audio files and archive files

I. Hosted workspace

Online workspace in the Cloud.

J. Microsoft 365 Copilot /Azure

Cloud services from Microsoft for Working Online.

K. Google Apps

Cloud services for Online Working.

L. Web hosting

Domain registration, mail forwarding and web space for business hosting. No maintenance on the website itself.

M. VoIP

Calling via the Cloud via SIP or Online telephone exchange.

N. Backup

backup copy of data to offsite, offline or online location.

O. Colocation

Customer equipment or Private or Public Cloud services served from data center.

P. Internet services

Infra for your IT environment to send/receive data from A to B.

Q. Hosted Desktop

Online desktop with applications in the Cloud.

R. VPS

A Virtual Private (web) Server (VPS) in the Cloud.

S. MDR

24/7 security monitoring, advanced cyber threat prevention, detection, and mitigation, plus targeted, risk-based thread hunting by a Managed SOC.

T. Security Awareness

To prevent data breaches, this service offers an e-learning program for employees and phishing simulations.

U. Central Management Systems

For the central management of NAS systems, firewalls and access points.

V. Dark Web Monitoring

24/7 human and machine monitoring of the dark web to see if credentials have been leaked.

W. MFA

Services for logging in with MFA.

X. SaaS Monitoring

Using machine learning, detect anomalies in user behavior in SaaS applications.

Y. **Automated Pentest**
The automatic detection of vulnerabilities in the network, both from the outside and from the inside.

Z. **Professional Service Automation tool**
Lucas IT uses a PSA system for CRM, Project Management, Service Desk and SLA management, among other things.

AA. **Newsletter system**
For sending newsletters.

BB. **Central signature software**
Signature software for e-mail signatures

CC. **Internet services**
Internet services in Cogas, Ziggo, KPN and Caiway area.

DD. **Credentials Management System**
For secure storage of credentials, device and/or network information by Lucas IT

EE. **Password vault**
Own online vault to store passwords.

FF. **Managed Wi-Fi controller**
For centrally managing Wi-Fi access points

5. Intended Use

The services listed in point 3 are designed and configured to process the following types of data: E-mail messages, Calendar appointments, contacts, e-mail data, text files, photo files, video files, audio files and archive files.

These services do not take into account the processing of special personal data, or the processing of data relating to criminal convictions and offences. Processing of this data with the service described above by the Client is at the Client's own discretion.

6. Processor uses the Data Pro Standard Clauses for its own processing agreement, which on https://www.lucasit.nl/avg can be found.

7. The Processor processes the personal data of its clients within and outside the EU/EEA.

8. The Processor uses the following sub-processors:

For the security of our services, the privacy of our customers and competitively sensitive information, our sub-processors are anonymized. If you, as a client, would like to have access to the sub-processors for the services you purchase from us, you can contact us by telephone on 0546-442322, or by e-mail via privacy@lucasit.nl. The processor may charge for this.

- **Microsoft (within EU/EEA)**
  Lucas IT uses this sub-processor to offer Microsoft cloud services, among other things. The data processed through Microsoft is processed within the European Union.
- **Twin data center (within EU/EEA)**
  Most of our own cloud services are located in a Twin data center in Overijssel, the Netherlands. The data processed in this data center remains in Overijssel. The data center is certified for ISO 27001:2013, ISO 27017, ISO 27018, ISO 9001:2015, ISO 14001:2015 and NEN 7510:2017. It also has a SOC2 certificate.
- **AntiSpam & ATP SAAS (within EU/EEA)**
  Data may be processed by our sub-processors Antispam & ATP SAAS. These parties process data within the EU/EEA.
- **Newsletter system (outside EU/EEA)**
  Lucas IT's newsletters are processed by our sub-processor Newsletter System. This sub-processor processes data in the United States. To ensure the European security and privacy level, the newsletter system conforms to the EU-U.S. Privacy Shield.
- **Internet providers (within EU/EEA)**
  Internet services in Cogas, Ziggo, KPN and Caiway area.
- **Broadband network in the Netherlands and Germany (within EU/EEA)**
  Internet services for business connectivity. This party is based in the Netherlands.

- **Central signature software (within EU/EEA)**
  Signature software for e-mail signatures is located within the EEA.
- **Professional Service Automation tool (outside EU/EEA)**
  Lucas IT uses a PSA system for CRM, Project Management, Service Desk and SLA management. This sub-processor processes data in the United States, among other places. To ensure the European level of security and privacy, the PSA conforms to BCR (Binding Corporate Rules and the EU-U.S. Privacy Shield.
- **Online support service (within EU/EEA)**
  Online tool for live support (remote support) of customers. The sub-processor is based in Germany.
- **Google (outside EU/EEA)**
  This sub-processor processes data in the United States, among others. To ensure the European security and privacy level, Google conforms to the EU-U.S. Privacy Shield.
- **Cloud Antivirus (within EU/EEA)**
  Lucas IT uses a sub-processor Cloud Antivirus within the EEA for antivirus protection and Cloud Antivirus service.
- **Endpoint Management and Remote Monitoring System (outside EU/EEA)**
  Lucas IT uses a sub-processor for Endpoint Management and Remote Monitoring System (RMM) for monitoring endpoints. This sub-processor processes data in the United States, among other places. To ensure the European security and privacy level, the Endpoint Management and Remote Monitoring System conforms to the EU-U.S. Privacy Shield.
- **Credentials Management System (outside EU/EEA)**
  Lucas IT uses this sub-processor for secure storage of credentials, device and/or network information. This sub-processor processes data in Canada. To ensure the European security and privacy level, the Credentials Management System conforms to the SOC2.
- **Hosted workspace (within EU/EEA)**
  Lucas IT uses this sub-processor to offer a hosted workspace in the Cloud. The sub-processor is established in the Netherlands.
- **Cloud Hosting Platform Manager (within EU/EEA)**
  Lucas IT uses this sub-processor to offer Virtual Private Servers (VPS). This sub-processor has an office within the European Union (EU) and processes data from cloud solutions in Amsterdam (AMS).
- **Cloud Hosting Platform and Domain Registration Service (within EU/EEA)**
  Lucas IT uses this sub-processor to offer web hosting and domain registration. This sub-processor processes data from solutions in Amsterdam (AMS). The sub-processor is established in the Netherlands.
- **Managed SOC (Within EU/EEA)**
  Lucas IT uses this sub-processor to offer MDR. A sub-processor within EEA.
- **Security Awareness (outside EU/EEA)**
  Lucas IT uses this sub-processor to offer e-learning and phishing simulations. This sub-processor processes data in the United States, among other places. To ensure the European security and privacy level, Security Awareness conforms to BCR (Binding Corporate Rules and the EU-U.S. Privacy Shield.
- **Dark Web Monitoring (outside EU/EEA)**
  Lucas IT uses this sub-processor to offer Dark web monitoring This sub-processor processes data in the United States, among others. To ensure the European level of security and privacy, Dark Web Monitoring conforms to BCR (Binding Corporate Rules and the EU-U.S. Privacy Shield.
- **SaaS Monitoring (outside EU/EEA)**
  Lucas IT uses this sub-processor to offer SaaS Monitoring. This sub-processor processes data in the United States, among other places. To ensure the European level of security and privacy, Dark Web Monitoring conforms to BCR (Binding Corporate Rules and the EU-U.S. Privacy Shield.
- **Automated Pentest (outside EU/EEA)**
  Lucas IT uses this sub-processor to offer an Automated Pentest. This sub-processor processes data in the United States, among other places. In order to guarantee the European level of security and privacy, Automated Pentest conforms to BCR (Binding Corporate Rules and the EU-U.S. Privacy Shield.
- **Managed Wi-Fi controller (outside EU/EEA)**
  Lucas IT uses this sub-processor to offer Managed Wi-Fi controller. This sub-processor processes data in the United States, among other places. To ensure the European level of security and privacy, the Managed Wi-Fi Controller conforms to BCR

(Binding Corporate Rules and the EU-U.S. Privacy Shield.

9. The Processor shall support the Client in the following manner in the event of requests from data subjects:

The Client may notify the Processor of a request for support, access requests, correction requests, deletion requests and data portability requests from a data subject to the Client by e-mail via privacy@lucasit.nl. The client must provide the processor with information about: the data subject, the type of request and the systems, databases and services involved. The processor makes a decision about the approval of the request, after which the client's contact person is then informed by e-mail about the decision, in the event negative with substantiation of the decision, and the possible follow-up steps of support if applicable. Read more in article 7.1.

10. After termination of the agreement with a Client, the Processor will in principle delete the personal data that it processes for the Client within three months in such a way that it can no longer be used and is no longer accessible (render inaccessible).

The data is overwritten many times by means of overwriting with new data.

11. After termination of the agreement with the Client, the Data Processor may, upon request, return all personal data that it processes for the Client within 4 weeks in the following manner:

If the service in question allows it, the client can make an export via the service. The export option is available up to 4 weeks after termination of the agreement. After that, the data is deleted. On request, the data can be securely transferred digitally in a suitable format or personally handed over via a data carrier in the format of the zip archive. Costs will be charged for handing over data on request. The costs charged for a request for the handing over of the data are the costs of the data carrier, transmission and the actions to be performed.

SECURITY POLICIES

12. The Processor has taken the following security measures to secure its service(s):

- complying with the confidentiality obligation referred to in Article 5 of the Data Pro Standard Clauses for Processing;
- the employees, who work with personal data, have a confidentiality agreement in a signed employment contract and additional rules of conduct in a separate terms of employment regulations;
- applying encryption to storage of sensitive data (if applicable and requested);
- using patch management to keep servers, network equipment, desktops and mobile devices up-to-date (if applicable and requested);
- the use of a role and access management, whereby only the persons assigned by the processor have access to sensitive data;
- Administrator/management accounts, may only be provided at the request of customer from the board/management processor, to the board/management end customer;
- the use of internally separated networks by means of VLANs or DMZ;
- deploying and maintaining software-based security (antivirus, anti-ransomware, firewall, etc.) and physical IT security systems (next-generation firewalls);
- training employees on information security awareness;
- internally, the processor has applied camera surveillance, key management, motion detectors and alarm system with certification;
- Internally, the processor uses individual usernames, passwords and multi-factor authentication, with appropriate password policies, secure VPN tunnels and encryption of external data systems. Access to systems is logged;
- documents containing sensitive information are destroyed by a professional archive shredder;
- the processor makes a selection in advance based on its own research into the sub-processor;
- the processor has (if applicable and requested) separated the production system from the development, test and acceptance system;
- On special request and at an additional cost, the customer can use a certified 'data erase' service.

13. The Processor has conformed to the following Information Security Management System (ISMS):

- The processor sets ISO 27001 and NEN7510 as a guideline for the IT services.
- The data center that Lucas IT uses for its services applies the following ISMS: ISO 27001:2013, ISO 27017, ISO 27018, ISO 9001:2015, ISO 14001:2015 and NEN 7510:2017. Also a SOC2 statement.
- Microsoft applies the following ISMS to its data center: ISO 27001:2022, ISO 27017:2015, ISO 27018:2019, ISO 27701:2019, ISO 22301:2019 and FedRAMP.

14. Processor has the following certifications

- The processor is currently active with the certification for ISO 27001:2022 and NEN 7510.

DATALEKPROTOCOL

15. In the event that something does go wrong, the Processor shall use the following data breach protocol to ensure that the Client is aware of incidents:

The processor uses monitoring tools to identify potential security incidents. If you, as a client, would like to have access to the monitoring tools for the services you purchase from us, you can contact us by telephone on 0546-442322, or by e-mail on privacy@lucasit.nl.

By using these monitoring tools, all systems (hardware, software, cloud) are linked to one central monitoring environment. The monitoring tool automatically processes the output of these systems based on predetermined filters and properties, after which the monitoring tool notifies alerts.

There is a procedure for reporting incidents internally. If the processor discovers a data breach in its organisation or the organisation of the controller, the processor will inform its client as soon as possible, by contacting the client's contact person, by sending an email from privacy@lucasit.nl to this contact person. The processor shall provide as much (if any) relevant data as possible, including:

- the description of the incident;
- the nature of the infringement;
- nature of (categories of) personal data of data subjects;
- estimation of the number of data subjects involved;
- the databases that may be affected;
- indication when the incident occurred;
- contact details of the contact person (DPO) (where can the controller go with questions?);
- Possible consequences (what can happen, what should the controller or data subject be aware of, point to the possibilities of identity fraud if data such as social security numbers, login and password details, passport copies, etc. have ended up in the wrong hands);
- Measures taken (what has the processor done to limit any damage or prevent it in the future?); and
- Measures to be taken by the controller or data subjects involved (what can data subjects do themselves, e.g. "keep an eye on mail, change passwords").

Reports of incidents are made to the client within 24 hours if possible. The processor itself will not report to the AP or data subjects. Whether or not to report remains the responsibility of the controller. If desired, the processor will support the client or the controller in the notification process.

PART 2: STANDARD PROCESSING CLAUSES

ARTICLE 1. DEFINITIONS

The following terms have the following meanings in these Standard Clauses for Processing, in the Data Pro Statement and in the agreement:

1.1 **Dutch Data Protection Authority (DPA):** supervisory authority, as described in Article 4(21) of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Processor**: party that, as an ICT supplier, processes Personal Data as a processor on behalf of its Client in the context of the performance of the Agreement.

1.4 **Data Pro Statement**: statement by the Processor in which it provides information regarding the intended use of its product or service, security measures taken, sub-processors, data breaches, certifications and dealing with the rights of Data Subjects.

1.5 **Data subject**: an identified or identifiable natural person.

1.6 **Client:** party on whose behalf the Processor processes personal data. The Client can be both a controller and another processor.

1.7 **Agreement**: the agreement applicable between the Client and the Processor, on the basis of which the ICT supplier provides services and/or products to the Client, of which the processing agreement forms part.

1.8 **Personal data**: all information about an identified or identifiable natural person, as defined in Article 4(1) of the GDPR, which the Processor processes in the context of the performance of its obligations arising from the Agreement.

1.9 **Data Processing Agreement**: these Standard Clauses for Processing, which together with the Data Pro Statement (or similar information) of the Processor form the Data Processing Agreement as referred to in Article 28(3) of the GDPR.

ARTICLE 2. GENERAL

2.1 These Standard Processing Clauses apply to all processing of Personal Data carried out by the Processor in the context of the delivery of its products and services and to all Agreements and offers. The applicability of the Client's processing agreements is expressly rejected.

2.2 The Data Pro Statement, and in particular the security measures contained therein, may be amended by the Processor from time to time to take account of changing circumstances. The Processor shall inform the Client of significant adjustments. If the Client cannot reasonably agree to the adjustments, the Client is entitled to terminate the processing agreement in writing within 30 days of notification of the adjustments, stating reasons.

2.3 The Processor processes the Personal Data on behalf of and on behalf of the Client in accordance with the written instructions of the Client agreed with the Processor.

2.4 The Client, or its client, is the controller within the meaning of the GDPR, has control over the processing of the Personal Data and has determined the purpose and means of the processing of the Personal Data.

2.5 The Processor is a processor within the meaning of the GDPR and therefore has no control over the purpose and means of the processing of the Personal Data and therefore does not make any decisions about, among other things, the use of the Personal Data.

2.6 The Processor shall implement the GDPR as laid down in these Standard Clauses for Processing, the Data Pro Statement and the Agreement. It is up to the Client to assess, on the basis of this information, whether the Processor offers sufficient guarantees with regard to the application of appropriate technical and organisational measures to ensure that the processing meets the requirements of the GDPR and that the protection of the rights of Data Subjects is sufficiently guaranteed.

2.7 The Client guarantees to the Processor that it acts in accordance with the GDPR, that it adequately secures its systems and infrastructure at all times and that the content, use and/or processing of the Personal Data are not unlawful and do not infringe any rights of a third party.

2.8 An administrative fine imposed on the Client by the AP cannot be recovered from the Processor, unless there is intent or deliberate recklessness on the part of the Processor's management.

ARTICLE 3. SECURITY

3.1 The Processor shall take the technical and organisational security measures as described in its Data Pro Statement. In taking the technical and organisational security measures, the Processor has taken into account the state of the art, the implementation costs of the security measures, the nature, scope and context of the processing, the purposes and intended use of its products and services, the processing risks and the risks that vary in likelihood and severity for the rights and freedoms of Data subjects that it has in view of the intended use of its products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the Processor's product or service is not designed for the processing of special categories of Personal Data or data relating to criminal convictions or offences or personal numbers issued by the government.

3.3 The Processor strives to ensure that the security measures to be taken by it are appropriate for the intended use of the product or service by the Processor.

3.4 In the opinion of the Client, the described security measures offer, taking into account the factors referred to in Article 3.1, a level of security appropriate to the risk of the processing of the Personal Data used or provided by it.

3.5 The Processor may make changes to the security measures taken if, in its opinion, this is necessary to continue to provide an appropriate level of security. The Processor will record important changes, for example in an amended Data Pro Statement, and will inform the Client of those changes where relevant.

3.6 The Client may request the Processor to take further security measures. The Processor is not obliged to make changes to its security measures at such a request. The Processor may charge the Client for the costs

associated with the changes made at the Client's request. Only after the amended security measures desired by the Client have been agreed in writing and signed by the Parties, the Processor will be obliged to actually implement these security measures.

ARTICLE 4. PERSONAL DATA BREACHES

4.1 The Processor does not guarantee that the security measures are effective under all circumstances. If the Processor discovers a Personal Data breach (as referred to in Article 4(12) of the GDPR), it will inform the Client without unreasonable delay. The Data Pro Statement (under data breach protocol) sets out how the Processor will inform the Client about breaches in connection with Personal Data.

4.2 It is up to the controller (Client, or its client) to assess whether the Personal Data breach of which the Processor has informed should be reported to the AP or Data subject. The notification of Personal Data breaches, which must be reported to the AP and/or Data subjects pursuant to Articles 33 and 34 of the GDPR, remains the responsibility of the controller (Client or its client) at all times. The Processor is not obliged to report personal data breaches to the AP and/or the Data Subject.

4.3 If necessary, the Processor will provide further information about the Personal Data breach and will cooperate with the necessary provision of information to the Client for the purpose of a notification as referred to in Articles 33 and 34 of the GDPR.

4.4 The Processor may charge the Client for the reasonable costs it incurs in this context at its then current rates.

ARTICLE 5. CONFIDENTIALITY

5.1 The Processor guarantees that the persons who process Personal Data under its responsibility have a duty of confidentiality.

5.2 The Processor is entitled to provide the Personal Data to third parties if and insofar as disclosure is necessary pursuant to a court decision, a statutory provision or on the basis of an authorised order issued by a government agency.

5.3 All access and/or identification codes, certificates, information regarding access and/or password policy provided by the Processor to the Client and all information provided by the Processor to the Client that gives substance to the technical and organizational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be made known to authorized employees of the Client. The Client shall ensure that its employees comply with the obligations under this article.

ARTICLE 6. TERM AND TERMINATION

6.1 This processing agreement is part of the Agreement and any new or further agreement arising from it, enters into force at the time the Agreement is concluded and is concluded for an indefinite period of time.

6.2 This Data Processing Agreement ends by operation of law upon termination of the Agreement or any new or further agreement between the parties.

6.3 In the event of termination of the processing agreement, the Processor shall, within the period included in the Data Pro Statement, delete all Personal Data in its possession and received from the Client in such a way that it can no longer be used and is no longer accessible (*render inaccessible*), or, if agreed, return it to the Client in a machine-readable format.

6.4 The Processor may charge any costs it incurs in the context of the provisions of Article 6.3 to the Client. Further agreements on this can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if a statutory regulation prevents the Processor from removing or returning the Personal Data in whole or in part. In such a case, the Processor will only continue to process the Personal Data to the extent necessary under its legal obligations. The provisions of Article 6.3 also do not apply if the Processor is the controller within the meaning of the GDPR with regard to the Personal Data.

ARTICLE 7. RECHTEN DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA) EN AUDITRECHTEN

7.1 Where possible, the Processor will cooperate with reasonable requests from the Client that are related to the rights of Data subjects invoked by the Data subjects at the Client. If the Processor is approached directly by a Data Subject, it will refer them to the Client where possible.

7.2 If the Client is obliged to do so, the Processor will cooperate with a data protection impact assessment (DPIA) or a subsequent prior consultation as referred to in Articles 35 and 36 of the GDPR upon a reasonable request to that effect.

7.3 The Processor will cooperate with requests from the Client to delete personal data insofar as the Client is unable to carry this out itself.

7.4 If desired, the Processor can demonstrate compliance with its obligations under the Data Processing Agreement by means of a valid Data Pro Certificate or a certificate or audit report (Third Party Memorandum) at least equivalent to it from an independent expert, if it has such a certificate or audit report.

7.5 In addition, at the request of the Client, the Processor will make available all further information that is reasonably necessary to demonstrate compliance with the agreements made in this processing agreement. If the Client nevertheless has reason to believe that the processing of Personal Data does not take place in accordance with the processing agreement, it can have an audit carried out at the expense of the Client no more than once a year by an independent, certified, external expert who has demonstrable experience with the type of processing carried out on the basis of the Agreement. The audit will be limited to checking compliance with the agreements regarding the processing of the Personal Data as laid down in this Data Processing Agreement. The expert will have a duty of confidentiality with regard to what he finds and will only report to the Client that constitutes a shortcoming in the fulfilment of the obligations that the Processor has on the basis of this processing agreement. The expert will provide a copy of his report to the Processor. Processor may refuse an audit or instruction from the expert if, in its opinion, it violates the GDPR or other legislation or constitutes an impermissible breach of the security measures it has taken.

7.6 The parties will consult on the results in the report as soon as possible. The parties will follow up on the proposed improvement measures laid down in the report insofar as this can reasonably be expected of them. The Processor will implement the proposed improvement measures insofar as they are appropriate in its opinion, taking into account the processing risks associated with its product or service, the state of the art, the implementation costs, the market in which it operates, and the intended use of the product or service.

7.7 The Processor is entitled to charge the Client for the costs it incurs in the context of the provisions of this article.

ARTICLE 8. SUB-PROCESSORS

8.1 In the Data Pro Statement, the Processor has stated whether, and if so, which third parties (sub-processors or sub-processors) the Processor engages in the processing of the Personal Data.

8.2 The Client gives permission to the Processor to engage other sub-processors for the performance of its obligations arising from the Agreement.

8.3 The Processor shall inform the Client of a change in the third parties engaged by the Processor, for example by means of an amended Data Pro Statement. The Client has the right to object to the aforementioned change by the Processor. The Processor shall ensure that the third parties engaged by it commit themselves to the same level of security with regard to the protection of the Personal Data as the level of security to which the Processor is bound towards the Client on the basis of the Data Pro Statement.

ARTICLE 9. OTHER

These Standard Clauses for processing, together with the Data Pro Statement, form an integral part of the Agreement. All rights and obligations under the Agreement, including the applicable general terms and conditions and/or limitations of liability, therefore also apply to the Data Processing Agreement.