Custon GDPR Compliance & Security policy 2.0

Custon's main activity is to carry out a Customer Experience Management program for its for gaining insight into service performance and thereby increasing the quality of service and customer satisfaction through measures. Part of this activity is approaching end customers as well internally as externally on behalf of the client for collecting feedback. This feedback is then processed into KPI steering information and displayed in a dashboard environment that is available to designated staff of our clients.

Below is a description of how Custon deals with the aforementioned activities within the framework of the GDPR. Within the GDPR there are two entities:

Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"
Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

In the above definition our client is the Controller and Custon is the Processor.

As a processor Custon takes care that:

PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA

- The legal basis for each processing activity is documented. Article 6 (1) EU GDPR.
- The purpose for each processing activity is documented. Article 4 (2) EU GDPR.
- The received personal data is only processed for the purpose that was intended at the time. Article 4 (1) EU GDPR of collection meaning getting feedback from and create dashboards.
- The consent-collecting mechanisms require some action (e.g., ticking a box) or affirmative statement by the data subject.
- The processing **does not** involve special categories of data based on consent, where explicit consent must be obtained (e.g., in writing or verbally) from the data subject.

RIGHTS OF THE DATA SUBJECTS WHILE PROCESSING AND ACCESSING THEIR INFORMATION

- There is a process in place to respond to requests for access to information held about a data subject.
- There is a process in place to rectify/delete information about a data subject pursuant to a request.
- There is a process in place to allow a data subject to revoke consent for a particular processing activity at any time.
- When consent for a particular processing activity is revoked, there are processes in place to ensure processing is stopped, including any processing by third parties.

- There is a process in place to comply with requests to restrict the processing of data if requested by a data subject, including any processing by third parties.
- There is a process in place to comply with requests from a data subject to have their personal data transferred directly to another controller.
- There is a process in place to stop processing for direct marketing purposes when an objection is received.
- A representative within the European Union been designated as Data Processing Officer within Custon.

TRANSFERS OF DATA TO THIRD PARTIES

- All data transfers are documented, including cross-border transfers

PRIVACY NOTICES

- A privacy Notice is provided to data subjects no later than at the time information is collected from those data subjects.
- The Privacy Notice clearly specify how data subjects can exercise their rights under the GDPR.

DATA BREACHES

- A process is in place to ensure the appropriate Supervisory Authority (Dutch Data Protection Authority) is notified within 72 hours of a confirmed data breach.
- Agreements/contracts with third parties (Datacenter provider www.Leaseweb.com) specify that the third party has to notify you (the processor) without undue delay after becoming aware of a data breach or potential data breach involving personal data.
- Internal policies are in place defining what is considered to be a data breach and when and if notification to data subjects or Supervisory Authorities is required.
- A log is kept of all data breaches that occur, along with the effects and remedial actions taken.
- Assessments of processing activities are conducted by the relevant personnel to determine the data protection measures that should be in place, proportionate to the risks involved with the processing activity.
- Privacy is assessed at the beginning stages of development of any processing activity.
- Measures such as data minimization and pseudonymisation are implemented across all applicable organizational units.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

- Data Protection Impact Assessments (DPIAs) are completed for processing activities involving special categories of information, automated decision making, or profiling.
- DPIAs are completed prior to implementing new technologies, processes, or projects.

GDPR implementation

- Custon supports client in getting a valid legal basis by supporting the process that the data subject provides valid consent. This means client must explain explicitly, exactly and completely in simple language (in a privacy statement) what is done with personal information. Client also have to point people to their rights, such as being allowed to change data, view the file or even have it destroyed. Client should also point out the possibility of submitting a complaint to the supervisory authority, the Dutch Data Protection Authority.
- For Custon there is a legal base because processing is necessary for entering into or the performance of a contract.
- Nevertheless will Custon also act by explain explicitly, exactly and completely in simple language (in a privacy statement) what is done with personal information. Custon also will point people to their rights, such as being allowed to change data, view the file or even have it destroyed. Custon will also point out the possibility of submitting a complaint to the supervisory authority, the Dutch Data Protection Authority. This can be done in the email and survey in the footnote.
- After receiving response from customers regarding the valid legal basis of sharing the personal information, client will delete the records for which there is no valid legal basis of sharing the personal information from the file before it is sent to Custon. This activity can also be delegated to Custon meaning that Custon will delete the records for which no valid legal basis exists after the file is received.
- Custon advises client to send the periodic survey email address files encrypted with a password and sent the password separately by SMS.
- Custon will import the email address files in the system and after that destroy the files immediately.
- The imported file is located in an extremely safe datacenter managed by Leaseweb.
- In the data work processes, data processing and storage procedures we contractually cooperate with Leaseweb which in turn works closely with EY, EY CertifyPoint and ComSec Consulting, resulting in the ISO 27001, PCI DSS, SOC 1, HIPAA and NEN 7510 assurance reports and certificates that ensures our data work processes, data infrastructure, data processing and security which meets the latest standards. We use the following certifications in the processing and storage of our data: ISO 27001, SOC1, NEN 7510,PCI DSS.
- For data classification, incident response, security and remedial action reasons the client files are stored separately and are identifiable with source, root, purpose and destination tags.
- Data subjects can ask for immediately removal, transfer or deletion of their information.
- Email with an URL are send to client customers with a unique key so every data and feedback is logged and trackable for security reasons.
- The communication link on which the client customer send his feedback data is secured by SSL so there is a minimum change of data theft.
- In the sent mail is a checkbox for no longer receiving mail for surveying according GDPR standards..
- Received data is automatically processed into KPI dashboard material which can only be entered by a strong password policy. Custon demands that each password meets strict security standards and is regularly renewed.
- Received data is stored in an extremely safe datacenter managed by Leaseweb.
- On behalf of client a data retention policy can be implemented. At the moment the retention period is automatically set at three years.

To help our clients in the GDPR field and give the reassurance client need, in fact our subcontractor LeaseWeb employs independent third party auditors to certify that there systems and processes thus our systems and processes comply with all the latest industry standards. And you can find all the relevant LeaseWeb certifications and details of the assurance reports right here.

All vital aspects covered

Certifications and assurance reports ensure logical security, physical security, service deployment, customer support, incident management, change management, and operational resilience meet industry-leading standards.

Global recognition

ISO 27001, PCI DSS, SOC 1, HIPAA and NEN 7510 certifications/assurance reports and LeaseWeb's external audit partners are recognized all around the world.

Peace of mind

Rest assured that wherever you are in the world our subcontractor LeaseWeb has effective operational controls and meet stringent audit levels for data protection and availability.

Our clients need to demonstrate to their customers, shareholders and other stakeholders that they have the necessary compliance in place to counter concerns over issues like cybersecurity and business resilience. Our subcontractor LeaseWeb has worked closely with EY, EY CertifyPoint and ComSec Consulting to achieve ISO 27001, PCI DSS, SOC 1, HIPAA and NEN 7510 reports/certifications which assure you that our infrastructure, data handling and security meet industry-leading standards.

Here are the certifications and assurance reports we in cooperation with Leaseweb can trust on in our datacenter and datacenter related data working processes.

ISO 27001

The International Organization for Standardization (ISO) 27001:2013 is the international security standard used to benchmark the protection of sensitive data. The certification process was carried out by EY CertifyPoint and encompassed organizational security policies, personnel security, physical and environmental security, systems and network security, and business continuity management.

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) ensures the secure handling of sensitive information and is intended to help organizations proactively protect customer account data. The certification process was carried out by Comsec Consulting. As customer data is not monitor or accessible, applicability of the PCI/DSS certification is restricted to physical security access to customer equipment through a combination of management systems and physical access safeguards and procedures. The covered aspects of the PCI/DSS certification are: 9.1 to 9.4, 9.10, 10.6.1, 11.1.2, 12.1, 12.2, 12.4 to 12.10. The following data centers are PCI DSS certified:

- AMS-01
- AMS-10
- FRA-10
- WDC-01
- SIN-11
- HKG-10

SOC 1

Service Organization Controls (SOC) reports provide an examination of a description of the system(s) we operate on behalf of our clients that are relevant to their internal control processes. This audit process was carried out by EY. There are two types of reports: type I and type II, where type II adds an extended assertion and auditor's opinion on the operating effectiveness of your controls.

HIPAA

The Health Insurance Portability and Accountability Act sets out standards for security controls to protect health information stored or processed online. Although there is no specific HIPAA certification for service providers, EY has issued with a third party statement that recognizes the platform as being compliant with HIPAA's requirements that relate to our service blocks for logical and physical security, operational resilience, incident management, service deployment and change management. This enables customers to leverage our platform as part of their overall HIPAA compliance.

NEN 7510

NEN 7510 is the standard developed by the Nederlands Normalisatie Institute for information security in the health sector. A third party statement by EY has been received for compliance with the NEN 7510's requirements in connection to the service blocks for logical and physical security, operational resilience, incident management, service deployment and change management.

CISPE

As part of a strong commitment to GDPR compliance our datacenter products has been registered with the Cloud Infrastructure Service Providers in Europe association (CISPE). CISPE have created a code of conduct for Infrastructure-as-a-Service (IaaS) providers such as our subcontractor LeaseWeb to guide and verify GDPR compliance.

EU US Privacy Shield

The U.S. Department of Commerce International Trade Administration (ITA) have confirmed that all the necessary Privacy Shield Principles were duly adhered to. This certification demonstrates that adequate technical and organizational measures has been taken for the level of privacy protection as required under the GDPR legislation. Furthermore, our GDPR ready General Conditions and Privacy Statement contribute to the EU-US Privacy Shield Principles Certification.