Auditreport

Concerning dataprocessor agreement with:
Blue Idea
Borgergade 2
8600 Silkeborg

November 14. 2022

Table of content

Managements description of processing activity

The purpose of this description is to supply information to Blue Ideas customers and their stakeholders (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation (GDPR).

Additionally, the purpose of this description is to provide specific information on matters regarding the security of processing, technical and organisational measures, responsibility between data controllers (our customers) and processor (Lessor Group), and how the services offered can help support the data subjects' rights.

Application system in scope is: SMS-Service

Risk assessment

Blue Idea has assessed the risk level to "Low" related to the processing of personal data.

The system processes only few and ordinary personal data. The systems process no sensitive personal data.

Auditors statement

Scope

We were engaged to provide assurance about:

a) Blue Ideas description of services in accordance with the data processing agreement with costumers as data controllers per November 14. 2022
b) The design and operation effectiveness of controls related to the control objectives stated in the Description.

Our responsibilities and method

Our responsibility is to express an opinion on Blue Ideas Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We performed our test of controls by the following actions:

Method	General description
Inquiries/requests	Interview with appropriate personnel. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can meet the expected level of effectiveness when implemented.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Silkeborg, November 14. 2022

Vipindi, VAT no. DK-39891875

Brian Reinhold Jensen
Partner
DPO og ISO 27001 Auditor

Description of processing and scope

The Data Controller uses the SMS-Service system, which is owned and managed by Blue Idea, to send SMS messages.

The character of processing

The data processor's processing of personal data on behalf of the data controller deals exclusively with ordinary personal data.

Categories of personal data

Ordinary personal data, Name, e-mail address, address and phonenumber.

Categories of data subjects:

- Employees of the data controller
- Customers of the data controller

Practical measures

Appropriate technical and organizational measures have been implemented for secure processing of personal data.

Description of tests of controls

The specific controls tested, and the nature, timing, and results of those tests are listed in the section "Control objectives, controls, tests, and results".

Control objectives, controls, tests, and results

1. General principles for data processors			
No.	Control activity	Test performed	Result of test
1.1	A list of the company's processing activities in the role of data processor has been prepared.	Inspected Blue Ideas list of processing activities.	No significant deviations noted.
1.2	Sub-data processor agreements have been made and annual audit of sub-data processors is carried out.	Inspected sub-data processor agreements and audits. Request for scheduled audits	No significant deviations noted. During the period, a new system has been implemented for the annual cycle for GDPR-related controls. Not all planned checks are created in the system on the day of the inspection.
1.3	A list of data controllers has been drawn up for use in the event of a breach of data security.	Inspected list of data controllers and contact informations.	No significant deviations noted.
1.4	Internal instructions have been made for notifying data controllers in the event of a breach of data security.	Requested that there are instructions for notifying data controllers in the event of a breach of data security. Inspected that data controllers are notified in cases where there has been a data breach.	No significant deviations noted. There have been no recorded data breaches during the period.
1.5	There are written procedures which contain requirements that personal data may only be processed when there is an instruction/Data Processing Agreement	Inspected that there are formalized procedures that ensure that processing of personal data only takes place in accordance with instructions. Inspected that the procedures contain requirements for a minimum annual assessment of the need for updating, including changes in the data controller's instructions or changes in data processing. Inspected that procedures are up to date.	No significant deviations noted.

1.6	The data processor has carried out a risk assessment. The risk assessment is updated regularly, at least once a year.	Inspected that there are formalized procedures that ensure that the data processor carries out a risk assessment to achieve adequate security. Inspected that the risk assessment carried out is up to date and includes the current processing of personal data. Inspected that the data processor has implemented the technical measures that ensure adequate security in accordance with the risk assessment.	No significant deviations noted.
1.7	The data processor may only transfer personal data to third countries or international organizations on instructions from the data controller.	Inspected that the data processor has a comprehensive and up-to-date overview of transfers of personal data to third countries or international organizations	No significant deviations noted.

2. Technical security measures			
No.	Control activity	Test performed	Result of test
2.1	For the systems and databases used for the processing of personal data, anti-virus software or other measures are installed to prevent the execution of malicious code. Antivirus is continuously updated.	Inspected that antivirus software has been installed for the systems and databases used to process personal data. Inspected that antivirus software is updated on a computer via random sampling.	No significant deviations noted.
2.2	External access to systems and databases used for processing personal data is through a secured firewall.	Inspected that external access to systems and databases used for processing personal data only takes place through a firewall.	No significant deviations noted.
2.3	Access to personal data is isolated to users with a work-related need for this.	Inspected that there are formalized procedures for restricting users' access to personal data. Inspected that there are formalized procedures for follow-up that users' access to personal data is in accordance with their work-related needs.	No significant deviations noted.

2.4	Encrypted connection is used between client and server	Inspected that connection between client and server is encrypted.	No significant deviations noted.
2.5	Passwords are stored encrypted.	Inspected that passwords are stored encrypted in the database.	No significant deviations noted.
2.6	Personal information used for development, testing or the like is always in pseudonymized or anonymized form. Use is made solely to carry out the purposes of the person responsible in accordance with the agreement and on his behalf.	Requested that there are formalized procedures for the use of personal data for development, testing and the like, which ensure that the use only takes place in pseudonymized or anonymized form.	No significant deviations noted.
2.7	Procedures have been established for the deletion of the data controller's data upon termination of subscription.	Inspected that there are formalized procedures for processing the controller's data when processing of personal data ceases. Inspected by a sample of discontinued data processing during the declaration period, that there is documentation that the agreed deletion or return of data has been carried out.	No significant deviations noted.

3. Organizational security measures			
No.	Control activity	Test performed	Result of test
3.1	Business procedures have been drawn up for the creation and termination of employees' access to personal data. Employees' access to, and work-related needs for, personal data are regularly reassessed.	Inspected that there are formalized procedures for granting and terminating employees' access to systems and databases used for processing personal data. Requested for resignations during the period and associated off-boarding procedure.	No significant deviations noted.
3.2	A data protection policy has been drawn up. The policy is communicated to employees. The policy is reviewed annually.	Inspected the staff handbook. Requested that there are procedures for communication to employees and annual review of the policy.	No significant deviations noted.

3.3	All employees are subject to confidentiality. The duty of confidentiality also applies after the employee's resignation. All employees are introduced to the data protection policy.	Inspected by a sample of 1 newly hired employee during the declaration period, that the employees in question have signed a confidentiality agreement. Inspected by a sample of 1 newly hired employee during the declaration period that the employees in question have been introduced to: • The information security policy • Procedures regarding data processing, as well as other relevant information	No significant deviations noted.
3.4	Upon resignation, processes have been implemented to ensure that the user's rights become inactive or cease, including that assets are confiscated.	Made request about procedures that ensure that the rights of resigned employees are deactivated or terminated upon resignation, and that assets such as access cards, PCs, mobile phones, etc. are confiscated. Inspected by a sample of 2 resigned employees during the declaration period that rights have been deactivated or terminated, and that assets have been seized.	No significant deviations noted.
3.5	Continuous awareness training is carried out for the data processor's employees in relation to IT security in general and processing security in relation to personal data.	Inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data. Inspected documentation that all employees who either have access to or process personal data have completed the offered awareness training.	No significant deviations noted. The company has introduced an online system for carrying out awareness activities.