PLAYABLE APS

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 JANUARY TO 31 DECEMBER 2023 ON THE DESCRIPTION OF THE PLAYABLE PLATFORM AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION.

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE 1 JANUAR TO 31 DECEMBER 2023 ON THE DESCRIPTION OF THE PLAYABLE PLATFORM AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Playable ApS
Playable ApS' Customers

Scope

We have been engaged to report on Playable ApS' (the Data Processor) description in section 3 of the Playable platform and Playable and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1 January to 31 December 2023.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is to express an opinion on the Data Processor's description in section 3 and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description, design and operating effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Pro-

cessor's description and about the design and operating effectiveness of the controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data Processor and described in section 2.

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

Limitations of Controls at a Data Processor

The Data Processor's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of Playable platform and Playable, that each individual Controller may consider important in their own environment. Also, because of their nature, controls at a Data Processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Data Processor's statement in section 2. In our opinion, in all material respects:

a. The description presents fairly Playable platform and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented for the period 1 January to 31 December 2023.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed for the period 1 January to 31 December 2023.

c. The technical and organisational measures and other controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 January to 31 December 2023.

Description of Test of Controls

The specific controls tested, and the results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended solely for data controllers who have used Playable platform, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 16. January 2024

BDO Statsautoriseret Revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Chef for Risk Assurance, CISA, CRISC

2. PLAYABLE APS' STATEMENT

Playable ApS processes personal data in relation to Playable platform and to our customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used Playable platform and Playable, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Playable ApS uses sub-processors. This sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

Playable ApS confirms that the accompanying description in section 3 fairly presents Playable platform and the related technical and organisational measures and other controls for the period 1 January to 31 December 2023. The criteria used in making this statement were that the accompanying description:

1. Presents Playable platform, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - The types of services provided, including the type of personal data processed.
    - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.
    - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
    - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects.
    - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
    - The controls that we, with reference to the delimitation of Playable platform would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.

2. Includes relevant information on changes in Playable platform and the related technical and organisational measures and other controls throughout the period.

3. Does not omit or distort information relevant to the scope of Playable platform and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Playable platform that the individual data controllers might consider important in their environment.

Playable ApS confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed for the period 1 January to 31 December 2023. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

3. The controls were applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1 January to 31 December 2023.

Playable ApS confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data Processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Aarhus, 16. January 2024

Playable ApS

Marianne Pharsen
COO

3. PLAYABLE APS DESCRIPTION OF THE SERVICE

PLAYABLE APS

Playable is a Danish-owned company developing and operating the "Playable platform". Playable's HQ is in Aarhus, Denmark with an additional sales office in Copenhagen, Denmark. Playable has three sales offices outside Denmark, companies located in Amsterdam, Netherlands and London, United Kingdom and a branch in Espoo, Finland (outside scope of ISAE3000).

Playable have approx. 75 employees who are specialised within system development, support, sales, marketing, and information security. They are organised in a development department, an operation and support department, a sales department, and a marketing department as well as a finance and legal department.

The finance and legal department controls Playables's security of personal data in relation to the processing that Playable handles on behalf of their clients, including entering into data processor agreements, replying to inquiries from the data controller, communication of personal data breach, compliance with internal policies and procedures, etc.

SERVICE AND PROCESSING OF PERSONAL DATA

The nature and extent of the Services
The Playable platform is a SAAS platform (app.leadfamly.com) provided by Playable to the Customer which is specified in the License Agreement between the parties.

The Playable platform
The Playable platform allows Customers to build campaigns using gamification. Gamification is defined as adding elements of game play (e.g., point scoring, competition with others, rules of play) to other areas of activity, and it is used as an online marketing technique to encourage engagement with a product or service.

The Playable platform has more than 25 different game concepts which includes a personality test, scratch card and wheel of fortune etc. The games are built and customised in the Playable platform by the Customer, but additional assistance from Playable can be purchased. The Playable platform has a large variety of features, both visual and integration-wise.

Data
Playable processes personal data on behalf of their clients, Playable is the Data Processor when they provide the Playable platform for the Customer who is Data Controller. Playable has entered into data processing agreements with the Controllers on this processing.

It is possible to collect data from the persons engaging with the campaigns built in the Playable platform. It is the Customer who decides which data to collect via the Playable platform, but it is usually data such as name and email address of the participant of the campaign game.

Playable has a high standard regarding data security and the company is ISO27001-certified. Playable uses Amazon Web Services in Ireland for hosting, and data is not transferred outside of the EU.

The personal data being processed fall within article 6 of the General Data Protection Regulation on ordinary personal data and may include personal name, e-mail, telephone number for identification, as well as in a few cases, confidential information, such as personal identification number included in article 11 (2) of the General Data Protection Regulation. It is the Data Controller who decides which information to process via the Playable Platform, however, an IP address will always be processed.

Integration and data transfer
Playable supports a large variety of integrations, including Hubspot, Salesforce, as well as integrations for statistical, storage and other purposes. The integration is usually made with the Customers own API or a WebHook.

Support
All inquiries should be sent to support@playable.com or through the chat in the platform. Playable provides operating support in the platform 8:00 – 21:00 GMT+1 during weekdays. If support is required in addition to this, it is individually priced.

More information
Information can be found at Playable website.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

Playable has prepared requirements for establishing, implementing, maintaining, and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the Controllers, good data processor practice, and relevant requirements for Data Processors in accordance with the General Data Protection Regulation and the Data Protection Act.

The technical and organisational security measures and other controls for protection of personal data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility together with compliance with current data protection legislation. Security measures and controls are wherever possible automated and technically supported by IT systems.

Management of the security of personal data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

DATA PROCESSOR AGREEEMENT	CONTROL AREA	ARTICLE
Control area A Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processor agreement.	• Entering into a data processor agreement with the Controller • Instruction for processing of personal data • Compliance with instruction for processing of personal data • Communication of unlawful instruction to the controller	• Art. 28, stk. 3 • Art. 28, stk. 3, litra a • Art. 29 • Art. 32, stk. 4 • Art. 28, stk. 10 • Art. 28 3, litra h
Control area B Procedures and controls are followed, which ensure that the data processor has implemented technical measures to ensure relevant processing security.	• Risk Assessment • Contingency plans in case of physical or technical incidents • Physical access control • Logical access control • Remote workplaces and remote access to systems and data • External communication connections • Encryption of personal data • Firewall • Anti-virus program • Vulnerability scanning and penetration testing. • Back-up and re-establishment of data • Logging in systems, databases, and network, including logging of application of personal data. • Monitoring • Testing, assessment, and evaluation of the efficiency of the technical and organisational security measures • Information security in development and changes • Segregation of development, test, and production environments • Personal data in development and test environments • Support assignments	• Art. 28 (3)(c) • Art. 25
Control area C	• Information Security Policy	• Art. 28(1)

DATA PROCESSOR AGREEEMENT	CONTROL AREA	ARTICLE
Procedures and controls are followed, which ensure that the data processor has implemented organizational measures to ensure relevant processing security.	• Review of the information security policy • Organisation of information security policy • Recruitment of employees • Resignation of employees • Training and instruction of employees processing personal data. • Awareness and information campaigns for employees • Confidentiality and secrecy agreement with employees • Obligations of security of processing and impact assessments. • Audit and inspection • Records of processing activities • Storage of the record • The Danish Data Protection Agency's access to the record	• Art. 28 (3)(b) • Art. 28 (3)(f) • Art. 28 (3)(h) • Art. 30 (2), (3) and (4) • Art. 33 (2) and (5) • Art. 38 • Art. 39
Control area E Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.	• Storage of personal data	• Art. 28 (3)(c)
Control objectives F Procedures and controls are followed, which ensure that only approved sub-data processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.	• Sub data processor agreement and instruction • Approval of sub data processors • Changes to approved sub data processors. • Overview of approved sub data processors • Supervision of sub data processors	• Art. 28 (2) and (4)
Control area H Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion, or restriction of information on the processing of personal data to the data subject.	• The data subject's rights	• Art. 28 (3)(e)
Control area I Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the data processor agreement entered into.	• Communication of personal data breach • Identification of personal data breaches • Registration of personal data breaches • Assisting the data controller with handling personal data breaches	• Art. 33 (2) • Art. 28 (3)(f)

RISK ASSESSMENT

It is Management's responsibility to take initiatives to address the threat scenario that Playable is facing at all times, so that the security measures and controls introduced are appropriate, and the risk of personal data breach, is reduced to a proper level.

The appropriate level of security is assessed on a current basis. The assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.

An annual risk assessment is performed as the basis of updating of the technical and organisational security measures and other controls. The risk assessment illustrates the probability and consequences of incidents that may threaten the security of personal data and thereby natural persons' rights and freedoms, including incidental, intentional, and unintentional events. The risk assessment considers the actual technical level and implementation costs.

Playable conducts two different risk assessments, where one has the company's data processing as its focus. The second assessment focuses on the company.

The first risk assessment focuses on the Playable platform and the data processed via the platform (Data for which Playable is processor) and serves to document the organisation's risk-based approach for selecting technical and organisational security measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (EU) 2016/679 of the European Parliament and of

the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information which entered into force on May 24, 2016, and applied on May 25, 2018 (the "GDPR"), article 24 inter alia.

Therefore, purpose of the risk assessment is to ensure that the procedures and the technical and organisational security measures implemented match the risks and the likelihood and severity for the rights and freedoms of the data subjects when the Playable platform processes personal data. Existing and already implemented security measures have been considered in the assessment of the relevant risk and threat categories. We refer to this for a more detailed explanation.

The risk assessment is updated at least once a year, or when relevant.

The second risk assessment describes and evaluates the company's risks regarding all relevant areas in the business units, such as the IT security, physical security, the employees' risk etc. This risk assessment will complement the above-mentioned risk assessment regarding the documentation of the risk assessments of the threat scenarios in Playable.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organisational security measures and other controls concern all processes and systems, which process personal data on behalf of the Controller. The control objectives and control activities stated in the control schedule are an integral part of the subsequent description.

The Data Processor's guarantees

Playable has introduced policies and procedures ensuring that Playable can provide the sufficient guarantees for completing appropriate technical and organisational security measures in such a way that the processing complies with the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights. Playable has established an organisation of the security of personal data as well as prepared and implemented an information security policy approved by Management, which is reviewed and updated on an ongoing basis. Procedures for recruiting and resignation of employees as well as guidelines for training and instruction of employees' processing personal data, including completion of awareness and information campaigns, exist.

Data processor agreement

Playable has introduced policies and procedures for entering into data processor agreements, which ensure that Playable in relation to the client contract enters into a data processor agreement, which states the terms for processing of personal data on behalf of the Controller. Playable applies a template for data processor agreements in accordance with the services to be provided, including information on the use of sub-processors. The data processor agreements are digitally signed and stored electronically.

Instruction for processing of personal data

Playable has introduced policies and procedures ensuring that Playable acts according to the instruction given by the Controller in the data processing agreement. The instruction is maintained with procedures instructing employees in how processing of personal data must be done, including who at the Controller may give binding instructions to Playable. Moreover, the procedures ensures that Playable informs the Controller when their instructions are not perceived to be following data protection legislation.

Sub-processors

Playable has introduced policies and procedures which ensure that sub-processors are assigned the same data protection obligations as stated in the data processor agreement between the Controller and Playable and that the sub-processor may give sufficient guarantees to protection of personal data. Procedures ensure that the Controller gives a preceding specific or general written approval of sub processors, including changes of approved sub processors are controlled.

Playable assesses the sub processor and their guarantees, before an agreement is entered into, to ensure that the sub-processor will be able to comply with the obligations assigned Playable. Playable monitors their sub processor on an annual basis based on a risk assessment of the specific processing of personal data by obtaining SOC2 auditor reports type 2, or similar documentation.

Confidentiality and professional secrecy

Playable has introduced policies and procedures ensuring confidentiality at the processing of personal data. All employees at Playable has committed to confidentiality by signing an employment contract containing terms of secrecy and confidentiality.

Technical and organisational security measures

Risk Assessment

Playable has completed the technical and organisational security measures based on an assessment of risk in connection to confidentiality, integrity, and availability. Please refer to separate section about this.

Contingency plans

Playable has established contingency plans, thus, Playable can re-establish the availability of and access to personal data in due time in case of physical and technical events. Playable has established emergency preparedness, which takes effect in these cases. Organisation of an emergency preparedness group is established and guidelines for activation of the emergency preparedness has been introduced.

Playable has designed contingency plans and plans for re-establishment of systems and data, which among other things ensure person independence in connection with activation of the emergency preparedness and the re-establishment. The plans are revised on a current basis in connection with changes to systems, etc.

Storage of personal data

Playable has introduced procedures ensuring that personal data are solely stored in accordance with the contract with the Controller and the list of locations in the accompanying data processing agreement.

Physical access control

Playable has introduced procedures ensuring that rooms are protected against unauthorised access. Only persons with a work-related or other legitimate need have access to the rooms, and special security measures have been taken for areas, where personal data is processed. Clients, suppliers, and other visitors must be registered and escorted.

Physical security

Playable has introduced procedures to control that servers are protected from unauthorized access, damage, outages, and similar incidents by special security measures used by the sub-processor. Servers are thus stored in a specially designed server room with physical and electronic access control and logging of accesses. The server room is protected against environmental threats such as fire, water intrusion, moisture, overheating, power failure and over-voltage. Systems for environmental protection of operating facilities are serviced and maintained on an ongoing basis in accordance with the regulations of the respective suppliers. The operating environment is monitored.

Logical access security

Playable has introduced procedures ensuring that access to systems and data are protected by an authorisation system. User is set up with unique user identification and password, and user identification is used in connection with allocation of resources and systems. All allocation of rights in systems is based on a work-related need. An assessment of the users' continued work-related need for access is reviewed at least once annually, including relevancy and correctness of allocated user rights. Procedures and controls support the process of creating, changing, and terminating users and allocated rights as well as review hereof.

The design of rules for i.a. length, complexity, regular changes to and history of password follows best practice for a secure logical access control. Technical measures have been established to support these rules with Single Sign on with 2FA for persons with access to personal data.

Remote workplaces and remote access to systems and data
Playable has introduced procedures ensuring that access from workplaces outside Playable premises and remote access to systems and data take places through VPN connections when working on server environments.

External communication connections
Playable has introduced procedures to ensure that external communications connections are secured with strong encryption and that email and other communications containing sensitive personal information are encrypted in the transmission using TLS minimum 1.2.

Encryption of personal data
Playable has introduced procedures ensuring that databases containing personal data are encrypted with AES 256 at rest and that the same apply for back-up copies.

Playable has introduced procedures ensuring that no personal data is stored on personal unit.

Algorithms and levels of encryption used for encryption of units, servers, and data are risk assessed on a current basis according to the current threat level.

Firewall
Playable has introduced procedures ensuring that traffic between the internet and the network is controlled by a firewall. External access by means of ports in the firewall is limited wherever possible, and access rights are allocated through actual ports for specific segments. Workstations uses firewall.

Network security
Playable has introduced procedures ensuring that networks in relation to use and security are divided into several virtual networks (VLAN), in which traffic between the individual virtual networks are controlled by firewalls. Servers with incorporated firewalls use this to ensure that access is only given to necessary services.

Anti-virus program
Playable has introduced procedures ensuring that units with access to networks and applications are protected against virus and malware. Antivirus programmes and other protective systems are continually updated and adjusted in relation to the actual threat level, and an ongoing monitoring of these systems has been set up, including periodical testing for functionality.

Vulnerability scanning
Playable has introduced procedures ensuring that a periodic port scanning for the purpose of identifying and prevent technical vulnerabilities in the infrastructure, thus, losses of confidentiality, integrity, and accessibility of systems and data are avoided. Vulnerability scans are performed by third party twice a year.

Penetration test
Playable has introduced procedures ensuring that a penetration test for the purpose of identifying and prevent technical vulnerabilities in the infrastructure, thus, losses of confidentiality, integrity, and accessibility of systems and data are avoided. Penetration tests are performed by third party once a year.

Back-up and re-establishment of data
Playable has introduced procedures ensuring that systems and data are backed up to prevent loss of data or loss of accessibility in the event of critical failures. Back-ups are protected with both physical and logical security measures, which prevent data from falling into the hands of unauthorised persons or that back-ups are destroyed by fire, water, malicious damage, or accidental damage.
Back-up is taken daily and saved for 14 days.

Maintenance of system software
Playable has introduced procedures ensuring that system software is updated regularly according to the suppliers' directions and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Logging in systems, databases, and network
Playable has introduced procedures ensuring that logging is set up in accordance with legislative requirements and business needs, based on a risk assessment of systems and the actual security alert status. The scope and quality of log data are sufficient to identify and demonstrate possible unauthorised use of systems or data, and log data is examined on a current basis for applicability and abnormal conduct. Log data is secured against loss and erasure.

Monitoring
Playable have introduced procedures ensuring that continuing monitoring of systems and technical security measures introduced.

Testing, assessment, and evaluation
Playable has introduced procedures for regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the processing security.

Data protection by design and by default

Playable has introduced policies and procedures for developing and maintaining the Playable platform, which ensure a controlled change of process. A change management system for controlling development and change tasks is applied, and every task follows a uniform process initiated by a risk assessment in accordance with the requirements of data protection by design and by default.

Development, testing, and production environments are separate, and segregation of duties is established between employees in the development department and the operation and support department. Each development and change task pass through a testing cycle and dummy-data are applied as test data. Procedures are introduced for version control, logging, and back-up. Thus, it is possible to reinstall previous versions.

Deletion and return of personal data.

System design is that Controllers must download all personal data in the "Playable platform" at the end of a campaign. If a controller terminates a contract Playable has no personal data to delete or return.

Assistance to the Controller

Playable has introduced policies and procedures ensuring that Playable can assist the Controller in complying with their obligation to reply to requests on executing the data subjects' rights. This is among other things done via a GDPR interface incorporated in the Playable platform.

Playable has introduced policies and procedures ensuring that Playable can assist the Controller in ensuring compliance with the obligations of article 32 on security of processing, article 33 on notification and communication of personal data breach, and article 34 - 36 on data protection impact assessment.

Playable has introduced policies and procedures ensuring that Playable can provide to the Controller all information necessary to demonstrate compliance with the requirements of the Data Processors. Besides,

Playable allows and assists in audits, including inspections performed by the Controller or others, who are authorised to do this by the Controller.

Records of processing activities

Playable has introduced policies and procedures ensuring that a record is kept of categories of processing activities performed on behalf of the Controller. The record is updated regularly and controlled during the annual review of policies and procedures, etc. The record is stored electronically and can be provided to the supervisory authority, by request.

Communication of personal data breach

Playable has introduced policies and procedures ensuring that personal data breaches are registered with detailed information about the event and that the Controller communicates without undue delay after Playable becomes aware of the personal data breach. The registered information makes the Controller able to assess whether the personal data breach must be reported to the supervisory authority and whether the data subjects should be notified.

Encryption of external communication

Playable has introduced procedures to ensure that external communications connections are secured with strong encryption and that email and other communications containing sensitive personal information are encrypted in the shipment using TLS.

Data protection responsible

Playable has appointed a Data Protection Responsible with the overall responsibility for data processing.

CHANGES DURING THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2023.

Playable has made the following significant changes to the service and the associated technical and organizational security measures and other controls during the period 1 January to 31 December 2023:

- Playable has implemented GuardDuty in June 2023; Amazon Web Services own intrusion detection system which monitors the VPC-flowlogs and set off alarms in case of abnormal activity and blocks suspicious activity.
- Playable has implemented Heysender in April 2023; An email sending service integrated in the Playable Platform to be used by the customers of the Playable Platform to send emails via the Platform. The service is optional.

COMPLEMENTARY CONTROLS WITH THE CONTROLLER

The Controller is obligated to implement the following technical and organisational security measures and other controls to reach the control objectives and thereby comply with the data protection legislation:

- The Controller is responsible for ensuring that the administrators' use of the Playable platform and the processing of personal data conducted in the system are in accordance with the data protection legislation.
- The Controller controls the user privileges in the Playable platform, including who are allocated administrator access and which rights the individual administrators are allocated.
- The data controller is responsible for ensuring that the administrators' use of the Playable platform and the processing of personal data carried out in the system takes place in accordance with data protection legislation.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has inspected procedures to obtain evidence of the information in Playable's description of the system, the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed or operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by Playable, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively for the period 1 January to 31 December 2023.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

With respect to the services provided by Amazon Web Service EMEA SARL within hosting, we have from independent auditor received the System and Organization Controls 2 (SOC 2) Type 2 Report for the sub-data providers' technical and organisational security measures and other controls for the period 2023.

For the services performed by heysender within hosting, we have from independent auditor received an ISAE 3000 type 1 report on sub-data providers' information security and measures in accordance with data processing agreement with Hey Group ApS customers at 12. October 2023.

These sub-processors' and service organisations' relevant control objectives and related controls are not included in Playable's description of the system and relevant controls related to operation of the system. Thus, we have solely assessed the reports and tested the controls at Playable, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Control area A		
Control Objective ▶ *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processor agreement entered into.*		
Control objectives	**Test performed by BDO**	**Result of test**
Entering into a data processor agreement with the Controller ▶ The Data Processor has procedures for entering into written data processor agreements which are in accordance with the services provided by the Data Processor. ▶ The Data Processor applies a data processor agreement template for entering into data processor agreements. ▶ When entering a written data processor agreement based on the data controllers' template, the data processor uses a checklist to ensure that it can comply with the data processor agreement. ▶ Data processor agreements are signed and stored electronically. ▶ Data processor agreements contain information about the use of sub data processors.	We have interviewed relevant personnel with the Data Processor. We have inspected Data Processor information security handbook and observed that there is a procedure for entering agreements with the services provided by the Data Processor. We have inspected Playable uses a template for entering into data processor agreements. We have inspected, by random sampling, and observed that data controller's agreements and instructions with customers use data processor template. We have observed that the data processors agreements are signed and stored electronically. We have inspected that data processor agreements contain information about use of sub data processors.	No exceptions noted.
Instruction for processing of personal data ▶ Data processing agreement contains instructions from data controller(s) ▶ The Data Processor obtains instruction for processing personal data from the Controller, in connection with entering into a data processor agreement.	We have interviewed relevant personnel with the Data Processor. We have inspected, by random sampling, and observed that a data processing agreement and related instructions have been entered into with customers who use the Playable platform.	No exceptions noted.

Control area A

Control Objective

- *Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processor agreement entered into.*

Control objectives	Test performed by BDO	Result of test
Compliance with instructions for processing of personal data ▶ The Data Processor solely processes personal data as per instruction from the Controller. ▶ The Data Processor has created and implemented written procedures regarding processing personal data to ensure that data is only processed based on instructions from data controllers. ▶ The Data Processor procedures are reviewed and updated regularly at least on a yearly basis. ▶ The Data Processor verifies that it complies with instructions in active data processing agreements.	We have interviewed relevant personnel with the Data Processor. We have inspected that the Data Processor solely processes personal data as per instruction from the controller, as described in data processors agreement template. We have inspected that the Data Processor has created and implemented written procedures regarding processing personal data, to ensure that data is only processed based on instructions from data controller. We have inspected that the Data Processor procedure is regularly looked over and updated, most recently in August 2023. We have inspected that Playable verifies that it complies with instructions in active data processing agreement.	No exceptions noted.
Communication of unlawful instructions to the Controller ▶ The Data Processor has prepared a procedure for communication to the Controller when the Controller's instruction is in contravention of the data protection legislation. ▶ The Data Processor communicates immediately to the Controller, if the Controller's instruction is in contravention of the data protection legislation.	We have interviewed relevant personnel with the Data Processor. We have inspected Data Protection Policy for Playable ApS as Data Processor and observed that Playable has a procedure for communication to the Controller when the Controller's instruction is in contravention of the data protection legislation. We have asked Playable if they have experienced illegal instruction during the declaration period, and Playable have not experienced illegal instruction during the declaration period.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Risk Assessment ▶ On an ongoing basis, risk assessment of potential risks for the accessibility, confidentiality and integrity of data is performed, in relation to the data subjects' rights and freedoms. ▶ The vulnerability of systems and processes is assessed based on identified threats. ▶ Risks are minimised based on the assessment of their likelihood and consequence. ▶ Risk assessments are updated on an ongoing basis when needed, but at least once a year.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has conducted two type of risk assessment for accessibility, confidentiality and integrity for Playable platform and AWS as a subcontractor. We have inspected that risk I based on the rights of the data subject. We have inspected that the risk assessments contain identified threats. We have inspected the risks are minimised based of their likelihood and consequence. We have inspected that the risk assessment has been assessed June 2023 as version 9 and approved by Management in November 2023.	No exceptions noted.
Contingency plans in case of physical or technical incidents ▶ The Data Processor has established a contingency plan, which ensures quick response time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. ▶ The Data Processor has established periodic testing of the contingency plan with a view to ensure that the contingency plans are up-to-date and efficient in critical situations. ▶ Tests of the contingency plans are documented and evaluated.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has established a contingency plan, which ensures quick response time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. We have inspected that the contingency plan has been tested, and therefore the contingency plan is up-to-date and efficient.	No exceptions noted.

Control area B

Control Objective

- *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*

Control objectives	Test performed by BDO	Result of test
Physical access control ▶ Physical access control is established, which has reduced the possibility for unauthorised access to the Data Processor's offices, facilities, and personal data. Only authorised personnel have access. ▶ All access is registered and logged. ▶ A regular and yearly control of the physical access security measures is performed.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for physical access control to Playable offices, facilities, and personal data. We have observed that in office hours it is possible to enter the facilities without any registration. Playable have established compensatory measures by defining that computer screens must be locked when leaving. Further, a screen lock is set to one minute and finally clean desk policies have been implemented. We have observed, by random sampling, that unmanaged desk is clean, and most computer screen locks were set to one minute.	We have observed that screen lock policy is defined in the procedure, but for one laptop the screen lock policy is not implemented in accordance with the determined policy. No further exceptions noted.
Logical access control ▶ The Data Processor has implemented procedures for user administration which ensures that user creation and deletion follow an uniform process and that all user creations are authorised. ▶ User rights are assigned based on work-related needs. ▶ Privileged user rights are assigned based on work-related needs. ▶ Users and user rights are reviewed at least once a year. ▶ The data processor has established logical access control for systems with personal information, including two-factor authentication. ▶ The data processor has established rules for password requirements, which must be followed by all employees as well as external consultants.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable have implemented procedure for user administration which ensures that user creation and deletion follow a uniform process and that all user creations are authorised. We have inspected that Playable have procedure for user rights are assigned based on work-related needs. We have inspected that Playable have procedure for privileged user rights are assigned based on work-related needs. We have inspected that Playable at least once a year reviews users, user rights and user activities.	We have observed that password policy is defined in the procedure, but for one laptop the password policy is not implemented in accordance with the determined policy. No further exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	We have inspected that Playable has established logical access control for systems with personal information, including two-factor authentication. We have observed, by random sampling, that most user's password was set according to the rules.	
Remote workplaces and remote access to systems and data ▶ Remote access to the Data Processor's systems and data is via an encrypted VPN connection. ▶ Remote access must go through two-factor authentication.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for access to the Data Processor's systems and that data is accessed via an encrypted VPN connection and via two-factor authentication.	No exceptions noted.
External communication connections ▶ External access to systems and databases, which are used to process personal data, is done through firewall and VPN. ▶ Exchange of personal data through e-mail is done by secure e-mail. ▶ External communication connections are encrypted.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for access to systems and databases, which are used to process personal data, is done through firewall and VPN. We have inspected that Playable has a procedure for using secure e-mail. We have inspected that Playable uses TLS1.2 for external communications.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Encryption of personal data ▶ The Data Processor has implemented an encryption policy for encryption of personal data. The policy defines the strength and protocol for encryption. ▶ Portable media with personal data are encrypted. ▶ When transmitting confidential and sensitive personal data via the internet and e-mail, encryption is applied.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for implementing an encryption policy for encryption of personal data. The policy defines the strength and protocol for encryption. We have inspected that Playable has procedures for encryption of portable media with personal data. We have observed that Playable uses encrypted transmission. It was not possible to test encrypted e-mail as it is only used for data controller requests.	No exceptions noted.
Firewall ▶ The Data Processor has configured firewall according to best practise.	We have interviewed relevant personnel with the Data Processor. We inspected that Playable has a procedure for configuration of firewall according to best practice. We have observed that the firewall is configured according to best practice.	No exceptions noted.
Anti-virus program ▶ Anti-virus software is installed on all servers and workstations. ▶ Anti-virus software is updated on an ongoing basis and updated with the latest version.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for using and configuring anti-virus.	We have observed that procedure for anti-virus is in place, but for one laptop antivirus is not installed. No further exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	We have inspected that Playable has procedure having antivirus installed and updated. We have observed, by taken samples, that workstations have installed anti-virus and updated.	
Vulnerability scanning and penetration testing. ▶ At least once a year, vulnerability scanning/port scanning of the Data Processor's network is performed. The result is documented in a report. ▶ The Data Processor reviews the report and follows up on ascertained weaknesses. ▶ The Data Processor processes/handles/mitigates any vulnerabilities based on a risk assessment. ▶ The Data Processor has documented their handling/mitigation of weaknesses found.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for vulnerability scan at least every half year and penetrations once a year. We have inspected that Playable has received a penetration test report for 2023, and there are no high vulnerabilities. We have inspected that Playable has a procedure for handling/mitigating any vulnerabilities based on a risk assessment. We have inspected that Playable has documented their handling/mitigation of weaknesses found.	No exceptions noted.
Back-up and re-establishment of data ▶ Back-up of systems and data is performed daily. ▶ Restore test is performed once a year.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for back-up of systems and data. We have inspected that Playable's backup of systems and data is performed daily. We have inspected that Playable does perform a restore test once a year.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Logging in systems, databases, and network, including logging of application of personal data. ▶ All successful and failed attempts to access the Data Processor's systems and data are logged. ▶ All user changes in systems and databases are logged. ▶ Logs are kept for 8 weeks.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for all successful and failed attempts to access the Data Processor's systems and that data are logged. We have inspected that Playable log all successful and failed access attempts. We have inspected Playable risk assessment regarding user change logs. We have been informed that user changes to personal data is not possible in the system. We have observed that Playable keeps logs for 8 weeks.	No exceptions noted.
Monitoring ▶ The Data Processor has established a monitoring system for monitoring of production environments, including uptime, performance, and capacity. ▶ The Data Processor is notified of identified alerts and follows up on these.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has established a monitoring system for monitoring of production environments, including uptime, performance, and capacity. We have observed that Playable receives alerts and follows up on the alerts.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Testing, assessment, and evaluation of the efficiency of the technical and organisational security measures ▶ The Data Processor tests, assesses and evaluates the efficiency of whether the technical and organisational security measures are appropriate in relation to the data handled on behalf of the Controller.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has tested, assessed, and evaluated the efficiency of whether the technical and organisational security measures are appropriate in relation to the data handled on behalf of the Controller.	No exceptions noted.
Development and sustainability of systems ▶ The Data Processor works on the basis of privacy-by-design principles in development and maintenance tasks. ▶ Risk assessment of system changes has been performed to ensure data protection through design and default settings.	We have made inquiries of relevant personnel at the Data Processor. We have inspected that Playable has a workflow for privacy by design in QA and production environments. We have inspected, by random sampling, that all changes are based on a risk assessment to ensure data protection.	No exceptions noted
Information security in development and changes ▶ The Data Processor works on security-by-design principles in development and change tasks. ▶ A rollback plan is implemented in case of errors in the production environment. ▶ User creation takes place as a starting point with the lowest user rights level. ▶ Only the Data Processor's developers have access to source code	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has an approved IT security policy. We have inspected that Playable has a procedure for a rollback plan. We have inspected that Playable has a procedure for creating only work-related user rights.	No exceptions noted

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	We have inspected that Playable has a procedure for segregation of duties. We have been informed that all developers have access to production environments.	
Segregation of development, test, and production environments ▶ Segregation of duties between development and operation has been introduced. ▶ Changes to functionality are tested before being put in operation. ▶ Development and test are performed in development environments, which are segregated from production systems. ▶ A version management system is used to register all changes in source code.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for segregation of duties. We have inspected that Playable has a procedure for testing changes to functionality before being put in operation. We have inspected that Playable has a procedure for functionality test before entering production. We have inspected that Playable has a procedure for segregation of development, QA, and production environments. We have inspected that Playable has a procedure for version management system to register all changes in source code.	Segregation of duties in software development processes are defined and followed, but due to the size of the organisation, Playable's Management has approved that developers have access to deploy software changes from development environment into production environment. No further exceptions noted.
Personal data in development and test environments ▶ Fictional test data or anonymised data are used in development and test environments.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure so fictional test data or anonymised data are used.	No exceptions noted.

Control area B		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Support assignments ▶ Supporters access to and handling of personal data is given based on support tickets and the support's work-related need.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for supporters' access and handling of personal data, which is given based on support tickets and the support's work-related need.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Information Security Policy ▶ The Data Processor has prepared and implemented an information security policy. ▶ The Data Processor has prepared and implemented a data protection policy.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has prepared and implemented an information security policy. We have inspected that Playable has prepared and implemented a data protection policy.	No exceptions noted.
Review of the information security policy ▶ The Data Processor's information security policy is reviewed and updated at least once a year. ▶ The Data Processor's data protection policy is reviewed and updated at least once a year.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable's information security policy is reviewed and updated at least once a year. We have inspected that Playable's protection policy is reviewed and updated at least once a year.	No exceptions noted.
Organisation of information security policy ▶ The Data Processor has documented and established management control of information security. ▶ The Data Processor has documented and established management control of the data protection policy.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has documented and established management control of information security. We have inspected that Playable has documented and established management control of data protection policy.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Recruitment of employees ▶ The Data Processor performs screening of potential employees before employment. ▶ The Data Processor performs background check in accordance with the Data Processor's procedure and the position, which the candidate is to take on.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for screening of potential employees' CVs before employment. We have inspected that Playable performs a screening of criminal records before employment. By random sampling, we have inspected employment contracts.	No exceptions noted.
Resignation of employees ▶ The Data Processor has prepared and implemented a procedure for resignation of employees at the end of the employment. ▶ At resignation, the employee is informed that the signed confidentiality agreement is still applicable.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for resignation of employees at the end of the employment. We have inspected that Playable informs the employee that the signed confidentiality agreement is still applicable.	No exceptions noted.
Training and instruction of employees processing personal data. ▶ The Data Processor conducts training of employees on an ongoing basis in accordance with data protection and information security and handling hereof.	We have interviewed relevant personnel with the Data Processor. We have inspected, that Playable conducts awareness training for employees on an ongoing basis in accordance with data protection and information security.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	We have inspected that Playable has a procedure for new employees so that they only get access to data in accordance with their protection and information security training.	
Awareness and information campaigns for employees ▶ The Data Processor performs information campaigns for employees on data protection and information security.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable performs campaigns for employees on data protection and information security.	No exceptions noted.
Confidentiality and secrecy agreement with employees ▶ All employees have signed an employment contract, which contains a section regarding confidentiality.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a contract template which contains a section regarding confidentiality. By random sampling, we have inspected signed contracts which all contains a section regarding confidentiality.	No exceptions noted.
Audit and inspection ▶ The Data Processor makes available the information necessary to the Controller and the supervisory authorities per request, in connection with audit and inspection of the Data Processor.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure which makes available the information necessary to the Controller and the supervisory authorities per request.	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	Upon request, we have been informed that there have been no requests for assistance to the data controller in relation to audit and inspection during the declaration period, which is why we have not been able to test for implementation and effectiveness.	
Records of processing activities ▶ The Data Processor has established a record of processing activities as Data Processor.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has established a record of processing activities.	No exceptions noted.
Storage of the record ▶ The record is stored electronically on the Data Processor's system/file drive.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable store the record electronically.	No exceptions noted.
The Danish Data Protection Agency's access to the record ▶ The Data Processor hands over the record at the request of the Danish Data Protection Agency.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for handing over the record at the request of Danish Data Protection Agency. Upon request, we have been informed that there have been no requests for the release of the record during the declaration	No exceptions noted.

Control area C		
Control Objective ▶ *Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
	period, which is why we have not been able to test for implementation and effectiveness.	

Control area D		
Control Objective ▶ *To ensure that the Data Processor can delete and return personal data when the service regarding the processing has terminated, in accordance with instruction from the Controller.*		
Control objectives	**Test performed by BDO**	**Result of test**
Deletion or returning of personal data. ▶ The Data Processor deletes or return the Controller's personal data per instruction, at termination of the main agreement.	We have interviewed relevant personnel with the Data Processor. We have been informed, at no Controller's has requested deletion or returning of personal data in the period.	No exceptions noted.

Control area E

Control Objective

- *Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*

Control objectives	Test performed by BDO	Result of test
Storage of personal data ▶ Personal data is contained so it is unavailable for unauthorised people. ▶ The Data Processor's personal data can only be accessed based on work-related needs. ▶ Confidential digital personal data is kept in encrypted format. ▶ Physical material containing personal data is kept sealed. ▶ Personal data is kept only as long as there is a legitimate reason for the use/storage.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for containing personal data, so it is unavailable for unauthorised people. We have inspected that Playable has a procedure for personal data only being accessed based on work-related needs. We have inspected that Playable has a procedure for encryption of data at rest. We have inspected that Playable has a procedure for keeping physical material with personal data sealed. We have inspected that Playable has a procedure for keeping personal data as long as there is a legitimate reason for the use/storage.	No exceptions noted.

Control area F		
Control Objective ▶ *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*		
Control objectives	**Test performed by BDO**	**Result of test**
Sub data processor agreement and instruction ▶ The data processor agreement with the sub data processor contains privacy information regarding data processors information.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable use AWS and heysenders as sub data processors. We have inspected the agreement of those sub processors including data processor agreements. We have inspected that new sub-processer have been informed to Controller in accordance with the agreement. We have inspected that agreement regarding data protection and storage of data are in accordance with agreed agreements within EU. Further, we have inspected that AWS has joined EU-U.S. Data Privacy Framework.	We have identified that AWS as a sub-processor has joined the new transfer basis EU-U.S. Data Privacy Framework, which entered into force on 10 July 2023. Playable has explained that there has been no transfer of personal data to unsafe third countries before 10 July 2023 or transfer to third countries after 10 July 2023. No further exceptions noted.
Approval of sub data processors ▶ The Data Processor only uses approved sub data processors.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable only uses approved sub data processor.	No exceptions noted.
Changes to approved sub data processors. ▶ The Data Processor has prepared an appropriate process with the Controller for change of approved sub data processors.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has prepared an appropriate process with the Controller for change of approved sub data processors.	No exceptions noted.

Control area F

Control Objective

- *Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.*

Control objectives	Test performed by BDO	Result of test
▶ The Data Processor communicates to the Controller when changing sub data processors in connection with general approval of sub data processor. ▶ The Controller may object to changing sub data processor. ▶ When changing sub data processor, the Data Processor must have a new preceding specific written approval from the Controller.	Upon request, we have been informed that there have been no changes of sub data processor during the declaration period, which is why we have not been able to test for implementation and effectiveness.	
Overview of approved sub data processors ▶ The Data Processor has an overview of approved sub data processors.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a list of approved subcontractors which the sub data processor (AWS) is part of.	No exceptions noted.
Supervision of sub data processors ▶ The Data Processor performs supervision, including obtains and reviews the sub data processor's audit opinions, certifications, etc. ▶ The Data Processor performs supervision of the sub data processor based on a risk assessment. ▶ The Data Processor performs supervision of the sub data processor at least once a year.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for supervision, including for obtaining and reviewing the sub data processor's audit opinions, certifications, etc. We have inspected that Playable performs supervision of the sub data processor based on a risk assessment at least once a year.	No exceptions noted.

Control area H

Control Objective

- *Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion, or restrictions of information on the processing of personal data to the data subject.*

Control objectives	Test performed by BDO	Result of test
The data subjects' rights ▶ The Data Processor has prepared a procedure for assistance to the Controller at fulfilling the data subjects' rights. ▶ It is possible to provide insight into all information registered in (system/service).	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for assistance to the Controller at fulfilling the data subjects' rights. Upon request, we have been informed that there has been no request to provide insight into any information during the declaration period, which is why we have not been able to test for implementation and effectiveness.	No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processor agreement.*		
Control objectives	**Test performed by BDO**	**Result of test**
Communication of personal data breach ▶ The Data Processor communicates to the Controller the personal data breach without undue delay. ▶ The Data Processor updates the Controller on all information relevant and necessary when the information is available to the Data Processor. ▶ Communication between Data Processor and Controller is documented and stored.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has a procedure for communicating to the Controller the personal data breach without undue delay. Upon request, we have been informed that there has been no personal breach during the declaration period, which is why we have not been able to test for implementation and effectiveness.	No exceptions noted.
Identification of personal data breaches ▶ The Data Processor performs surveillance for detecting breached on the personal data security. ▶ The Data Processor has prepared a procedure for assessing and identifying personal data breaches.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable has educated all personal to discover breaches of the personal data security. We have inspected that Playable has a procedure for assessing and identifying personal data breaches.	No exceptions noted.
Registration of personal data breaches ▶ The Data Processor registers personal data breaches in the data breach log. ▶ The Data Processor has prepared and implemented a procedure for experience gathering when personal data is breached.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable registers personal data breaches in a data breach log.	No exceptions noted.

Control area I		
Control Objective ▶ *Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processor agreement.*		
Control objectives	**Test performed by BDO**	**Result of test**
	We have inspected that Playable have implemented a procedure for experience gathering when personal data is breached.	
Assisting the data controller with handling personal data breaches ▶ Procedures for assistance to the Controller when assisting in relation to articles 33-34 and 36 have been prepared.	We have interviewed relevant personnel with the Data Processor. We have inspected that Playable have procedures to the Controller when assisting in relation to articles 33-34 and 36 have been prepared.	No exceptions noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-01-16 13:00:04 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2024-01-16 13:17:53 UTC

Marianne Sejr Pharsen
COO
Serienummer: 89535f13-0ab0-47cd-a825-75e2be02c00b
IP: 80.208.xxx.xxx
2024-01-17 08:58:14 UTC