INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 JANUARY TO 31 DECEMBER 2024 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

Playable ApS

BDO

CONTENT

1. INDEPENDENT AUDITOR'S OPINION 2

2. PLAYABLE APS' STATEMENT 5

3. PLAYABLE APS' DESCRIPTION OF THE PLAYABLE PLATFORM 7

Playable aps 7

service and processing of personal data 7

Management of the security of personal data 8

Risk Assessment 10

Technical and Organisational Security Measures and Other Controls 10

Changes during the period from 1 January to 31 December 2024 15

Complementary controls with the Controller 15

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS 16

Control Area A 18

Control Area B 20

Control Area C 26

Control area D 30

Control Area E 32

Control Area F 33

Control Area H 36

Control Area I 37

Control area J 39

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE 1 JANUARY TO 31 DECEMBER 2024 ON THE DESCRIPTION OF THE PLAYABLE PLATFORM AND PLAYABLE 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 2024.

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 Processor'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 the 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 2024.

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 2024.

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 2024.

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,24 January 2025

BDO Statsautoriseret Revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. PLAYABLE APS' STATEMENT

Playable ApS processes personal data in relation to Playable platform and Playable 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. These sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

Playable 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 2024. 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 authorized 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, unauthorized 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 2024. 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 2024.

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, 24 January 2025

Playable ApS

Marianne Pharsen
COO

3. PLAYABLE APS' DESCRIPTION OF THE PLAYABLE PLATFORM

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 Playable'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.playable.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 30 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. IP-addresses are always collected.

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:

CONTROL AREA	SUB-CONTROL AREA	GDPR ARTICLE
A - Processing of personal data on behalf of the data controller's instructions	A.1 - Procedure for processing personal data	Article 28(3)
	A.2 - Compliance with instructions for the processing of personal data	Article 28(3) and Articles 29 and 32(4)
	A.3 - Notification of the data controller in the event of an unlawful instruction	Article 28(3)(h)
	A.4 - Record of processing activities	Article 30(2), (3) and (4)
B - Technical measures	B.1 - Agreed security measures	Article 28(3)(c)
	B.2 - Risk assessment	Article 28(3)(c)
	B.3 - Antivirus	Article 28(3)(c)
	B.4 - Firewall	Article 28(3)(c)
	B.6 - Conditional access - access to personal data	Article 28(3)(c)
	B.7 - Monitoring of systems and environments	Article 28(3)(c)
	B.8 - Encryption in connection with the transmission of personal data	Article 28(3)(c)
	B.9 - Logging	Article 28(3)(c)
	B.10 - Anonymization of personal data in development tasks	Article 28(3)(c)
	B.11 - Vulnerability scans and penetration tests	Article 28(3)(c)
	B.12 - Maintenance of system software	Article 28(3)(c)
	B.13 - Conditional access - procedure and periodic review	Article 28(3)(c)
	B.14 - Logical access control	Article 28(3)(c)

CONTROL AREA	SUB-CONTROL AREA	GDPR ARTICLE
	B.15 - Physical access control	Article 28(3)(c)
	B.16 - Backup and restoration	Article 28(3)(c)
	B.17 - Remote workplaces and remote access to systems and data	Article 28(3)(c)
C - Organisational measures	C.1 - Information security policies and information security policy review	Article 28(1)
	C.2 - Information security policies in accordance with data processing agreements	Article 28(1)
	C.3 - Recruitment of employees - Screening	Article 28(1)
	C.4 - Recruitment of employees - Non-disclosure agreement with employees and introduction to information security	Article 28(1) and Article 28(3)(b)
	C.5 - Termination of employment - withdrawal of access rights and assets	Article 28(1)
	C.6 - Resignation of employees - information on confidentiality and professional secrecy	Article 28(1) and Article 28(3)(b)
	C.7 - Information security awareness, education and training	Article 28(1)
	C.8 - Supporter's access to personal data	Article 28(1)
D - Deletion of personal data	D.1 - Deletion of data in accordance with the controller's requirements	Article 28(3)(g)
	D.2 - Requirements for storage and deletion period of data are in accordance with the data controller's requirements	Article 28(3)(g)
	D.3 - Deletion and return upon termination of customer relationship	Article 28(3)(g)
E - Retention of personal data	E.1 - Retention of information is in accordance with the requirements of the data controller	Article 28(3)(c)
	E.2 - Location of processing and storage of information	Article 28(3)
F - Sub-processors	F.1 - Sub-data processing agreement and instructions	Article 28(2) and (4)
	F.2 - Approval of sub-processors	Article 28(2)
	F.3 - Changes in approved sub-processors	Article 28(2)
	F.4 - Obligations of the sub-processor	Article 28(2) and (4)
	F.5 - Overview of sub-processors	Article 30(2)
	F.6 - Supervision of sub-processors	Article 28(2) and (4)
H - Data Subject Rights	H.1 - Procedure for the enforcement of data subjects' rights	Article 28(3)(e)
	H.2 - Technical measures for the fulfilment of data subjects' rights	Article 28(3)(e)
I - Security Breaches	I.1 - Notification of personal data breaches	Article 33(2)
	I.2 - Identification of Personal Data Breaches	Article 33(2)
	I.3 - Timely notification of personal data breaches	Article 33(2)
	I.4 - Assistance to data controllers in the event of personal data breaches	Article 28(3)(f)
J - Data protection by design and default settings	J.1 - Change management and privacy-by-design	Article 25
	J.2 - Implementing change in the production environment	Article 25
	J.3 - Separation of the development, test and production environment	Article 25
	J.4 - Access to source code	Article 25

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 "general" risk assessment.

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. Risk assessments of Playable's AI systems has been done separately and has been included in the Playable AI Act Assessment.

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 auditor reports of the type ISAE 3000 or SOC 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 have 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.e. 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 programs 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 anonymized production 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 for 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 2024

Playable has made the following significant changes to the Playable platform and the associated technical and organisational security measures and other controls during the period 1 January to 31 December 2024.:

- Playable has reassessed Inmobile in 2024 and added it as a sub-processor;
  A text messaging service integrated in the Playable Platform to be used by the customers of the Playable Platform to send text messages via the Platform. The service is optional. However, some customers were already facilitating the use of this processor before it was classified as a sub-processor. Therefore, the relevant customers have been notified and have accepted Inmobile as a new sub-processor.
- Playable has also introduced a new cooperation with Truesec, a cyber security provider which will perform Vulnerability scans, Penetration tests and assist in other areas of IT-Security related areas. The collaboration is broader than the previous provider within cyber security.

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 TEST RESULTS

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 2024.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation and effectiveness hereof were 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 April 2023 to March 31, 2024.

For the services performed by Heysender within hosting, we have from independent auditor received an ISAE 3000 type 2 report on sub-data providers' information security and measures in accordance with data processing agreement with Hey Group ApS customers covering the period October 1 to September 30, 2024.

For the service performed by Inmobile, we have from independent auditor received an ISAE 3000 type 2 report on sub-data providers' information security and measures in accordance with data processing agreement with Inmobile ApS covering the period May 1, 2023 to April 30, 2024.

These sub-processors' and service organizations' 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 objectives *Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the entered into data processing agreement.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
A.1	**Procedure for processing personal data** There are written procedures that require that personal data may only be processed when there is an instruction. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there is a formalized procedure in place to ensure that the processing of personal data only takes place in accordance with instructions. We have inspected that the procedure includes a requirement for a minimum annual assessment of the need for updating, including changes in the data controller's instructions or changes in data processing. We have inspected that the procedure has been updated and management approved in October 2024.	No deviations were found.
A.2	**Compliance with instructions for processing personal data** The Data Processor only carries out the processing of personal data that is stated in the instructions from the Data Controller	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable uses a template for entering into data processor agreements. We have randomly inspected data processing agreements entered with data controllers and observed that the agreements contain instructions from data controllers. We have inspected the data processor's record of processing activities and randomly inspected that the processing takes place in accordance with instructions from the data controller. We have observed that the data processors agreements are signed and stored electronically.	No deviations were found.

Control Area A			
Control objectives *Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the entered into data processing agreement.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
A.3	**Notification of the data controller in the event of an illegal instruction** The data processor shall immediately notify the data controller if, in the opinion of the data processor, an instruction conflicts with the General Data Protection Regulation or data protection provisions in other EU law or the national law of the Member States.	We have carried out enquiry with appropriate personnel of 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. On request, we have been informed that there have been no cases during the declaration period where instructions have been assessed as contrary to legislation.	We have found that there have been no cases where instructions have been assessed as contrary to legislation. We have therefore not been able to test the control for implementation and efficiency. No deviations were found.
A.4	**Record of processing activities** The Data Processor has established a list of categories of processing activities as a Data Processor. The list must include: • the name and contact details of the data controller; • the categories of processing carried out on behalf of the controllers; • the name and contact details of each sub-processor; • indication of any transfer of personal data to a third country. The record shall be kept electronically and shall be made available to the supervisory authority upon request.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected the data processor's record of categories of processing activities as a data processor and observed that it contains relevant information and that the record is stored electronically. We have inspected that the listing has been updated and/or approved. On request, we have been informed that the Danish Data Protection Agency has not requested disclosure of the list during the declaration period.	We have established that the Danish Data Protection Agency did not request disclosure of the list at the time of the declaration. We have therefore not been able to test the control for implementation and efficiency. No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
B.1	**Agreed security measures** There are written procedures that require that agreed safeguards are put in place for the processing of personal data in accordance with the agreement with the data controller. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that formalized procedures are in place to ensure that the agreed security measures are put in place. We have inspected that procedures have been updated and approved in October 2024.	No deviations were found.
B.2	**Risk assessment** The data processor has carried out a risk assessment and, on the basis of this, implemented the technical measures that are deemed relevant to achieve appropriate security, including the establishment of the security measures agreed with the data controller.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the data processor has carried out a risk assessment based on potential risks to the accessibility, confidentiality and integrity of the data subject in relation to the rights of the data subject. We have inspected that the risk assessment carried out has been updated and approved. We have randomly inspected that the data processor has implemented technical measures based on the risk assessment, including measures agreed with the data controller.	No deviations were found.
B.3	**Antivirus** Antivirus is installed for the workstations and systems used for the processing of personal data, which is continuously updated.	We have carried out enquiry with appropriate personnel of the data processor. We have randomly inspected that for PCs used for the processing of personal data, antivirus has been installed that has been updated.	No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
B.4	**Firewall** External access to systems and databases used for the processing of personal data is done through a secured firewall.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the firewall is configured according to internal policy for this.	No deviations were found.
B.6	**Conditional access - access to personal data** Access to personal data is isolated to users with a work-related need for it.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable have an implemented procedure for user administration which ensures that user creation and deletion follow a uniform process and that all user creations are authorized. We have observed that Playable have a procedure to ensure that user rights are assigned based on work-related needs. We have inspected that the agreed technical measures support the maintenance of the restriction on users' work-related access to personal data. We have randomly inspected that users' access to systems and databases is limited to the employees' work-related needs.	No deviations were found.
B.7	**Monitoring of systems and environments** For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes: • Alerts from the monitoring system	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that systems and databases used for the processing of personal data have established system monitoring with alarms.	No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
B.8	**Encryption for the transmission of personal data** Effective encryption is used when transmitting confidential and sensitive personal data via the internet and by e-mail.	We have carried out enquiry with appropriate personnel of the data processor. We have observed 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 observed that Playable has procedures for encryption of portable media with personal data. We have observed that Playable applies encrypted transmission including VPN.	No deviations were found.
B.9	**Logging** Logging has been established in systems, databases and networks for the following conditions: o Changes to system privileges for users o Failed log-in attempts to systems, databases and networks	We have carried out enquiry with appropriate personnel of the data processor. We have observed 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 observed 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.	No deviations were found.
B.10	**Anonymization of personal data in development tasks** Personal data used for development, testing or the like is always in pseudonymised or anonymised form. Use is only to carry out the controller's purpose in accordance with the agreement and on the controller's behalf.	We have carried out enquiry with appropriate personnel of the data processor.	No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have observed that Playable have a procedure to ensure that data in development and test database are anonymized. We have randomly inspected in development and test databases that personal data in these databases is anonymized.	
B.11	**Vulnerability scans and penetration tests** The established technical measures are continuously tested by vulnerability scans and penetration tests.	We have carried out enquiry with appropriate personnel of 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 and a vulnerability report for 2024, 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 deviations were found.
B.12	**System Software Maintenance** Changes to systems, workstations, databases, and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected by extraction that databases and networks are updated with relevant updates and security patches. We have randomly inspected that workstations are updated with the latest system update.	No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
B.13	**Conditional Access - procedure and periodic review** There is a formalized procedure for granting and terminating user access to personal data. Users' access is regularly reviewed, including that rights can still be justified by a work-related need.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that formalized procedures are in place for granting and discontinuing users' access to systems and databases used for the processing of personal data. We have inspected Playable's periodic review procedure and observed that accesses are reviewed twice a year and that accesses are terminated upon resignation or changes We have observed that the employee's access to systems where personal data is processed has been approved and that the employee has a work-related need for the access. We have randomly inspected documentation for user reviews in October 2024.	No deviations were found.
B.14	**Logical access control** The data processor has established rules for password requirements that must be followed by everyone with access to personal data.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable have a procedure for establishing logical access control with MFA, as well as which users are using MFA. We have observed that Playable has established minimum password policy requirements depending on the system's criticality. We have randomly inspected that passwords were a minimum of 8 characters for users with access to personal data.	No deviations were found.

Control Area B			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
B.15	**Physical access control** Physical access security has been established so that only authorized persons can gain physical access to premises and data centres in which personal data is stored and processed.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that Playable have 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 randomly inspected, that unmanaged desk is clean, and most computer screen locks were set to one minute.	No deviations were found.
B.16	**Backup and restoration** The Data Processor has established a procedure for backup and re-establishment of data and systems that ensures that relevant systems and data are backed up and stored at another physical location, and that systems and data can be re-established.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable has a procedure for backing up systems and data. We have observed that Playable regularly performs backups of data. Upon request, we were informed and that Playable follows the guidelines from Amazon.	No deviations were found.

Control Area C			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
C.1	**Information security policies and information security policy review** The data processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment carried out. An assessment is made on an ongoing basis – and at least once a year – of whether the IT security policy needs to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected information security documents and observed that Playable has developed and implemented an information security policy, which is updated and approved at least annually. We have observed that Playable has developed and implemented a data protection policy. We have inspected the template for employment contracts and observed that Playable has developed a contract for new hires referencing the information security policy.	No deviations were found.
C.2	**Information security policies in accordance with data processing agreements** The data processor's management has ensured that the information security policy is not in conflict with the data processing agreements entered.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected documentation for the management's assessment that the information security policy generally meets the requirements for security measures and processing security in entered into data processing agreements.	No deviations were found.
C.3	**Recruitment of employees – Screening** A review of the data processor's employees is carried out in connection with employment. The verification shall include, where appropriate: • Criminal record	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there are formalized procedures in place to ensure verification of the data processor's employees in connection with employment.	No deviations were found.

Control Area C			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have randomly inspected that the data processor has carried out verification of candidates and that the tests have included relevant documentation.	
C.4	**Recruitment of employees - Non-disclosure agreement with employees and introduction to information security** Upon employment, employees sign a confidentiality agreement. Furthermore, the employee is introduced to information security policy and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.	We have carried out enquiry with appropriate personnel of the data processor. We have randomly inspected that employees have signed requirements for confidentiality in the employment contract. We have randomly inspected that employees have been introduced to: • Information security policy • Procedures relating to data processing, as well as other relevant information.	No deviations were found.
C.5	**Termination of employees - withdrawal of access rights and assets** Upon resignation, a process has been implemented by the data processor to ensure that the user's rights become inactive or cease, including that assets are confiscated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected procedures that ensure that the rights of resigned employees are inactivated or terminated upon resignation, and that assets such as access cards, PCs, mobile phones, etc. are confiscated. We have randomly inspected that for the resigned employee, rights have been deactivated or terminated, and that assets have been withdrawn in a timely manner.	No deviations were found.

Control Area C			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
C.6	**Resignation of employees - information about confidentiality and professional secrecy** Upon resignation, the employee is informed that the signed confidentiality agreement is still in force and that the employee is subject to a general duty of confidentiality in relation to the processing of personal data that the data processor performs for the data controllers.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected the template for resignation letters and observed that Playable informs the departing employee that the confidentiality agreement also applies after their departure. We have randomly inspected that for terminated employees, the data processor has informed the terminated employees that the imposed duty of confidentiality continues to apply after termination of employment.	No deviations were found.
C.7	**Awareness, education and training regarding information security** Ongoing awareness training is carried out of the data processor's employees in relation to IT security in general and processing security in relation to personal data.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data. We have observed that employees are offered ongoing training, and the most recent session was conducted in October 2024 We have inspected documentation that all employees who either have access to or process personal data have completed the offered awareness training.	No deviations were found.
C.8	**Supporter's access to personal data** The Data Processor has established procedures for supporters' access to personal data, which ensure that supporters' access and handling of personal data in connection with support tasks	We have carried out enquiry with appropriate personnel of the data processor.	No deviations were found.

Control Area C			
Control objectives *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
	is based on support tickets and the supporter's work-related needs.	We have inspected that there are formalized procedures in place to ensure that supporters' access and handling of personal data in connection with support tasks is based on support tickets and the supporter's work-related needs. We have randomly inspected support cases and observed that the procedure is being followed.	

Control area D			
Control objectives *Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
D.1	**Deletion of information in accordance with the data controller's requirements** There are written procedures that require that personal data is stored and deleted in accordance with the agreement with the data controller. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have observed that the system design of the platform allows the data controller to retrieve all personal data either continuously or at the latest upon the conclusion of a campaign. We have reviewed Playable's privacy policy procedure and observed that Playable has formalized procedures for data deletion and return. We have inspected the control report and deletion policy and observed that Playable has established policies for data deletion and reporting. We have observed that the deletion policy is regularly reviewed and was most recently updated in September 2024. Upon request, we have been informed that deletion is preformed according to the deletion policy.	No deviations were found.
D.2	**Requirements for the storage and deletion period of data are in accordance with the data controller's requirements** The following specific requirements have been agreed for the data processor's storage periods and deletion routines: • The Downloads folder on workstations is automatically deleted every month.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the available procedures for storing and deleting personal data contain specific requirements for the data processor's retention periods and deletion routines. We have inspected the data processors' random samples and observed that download folders on workstations are deleted once a month.	No deviations were found.

Control area D			
Control objectives *Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
D.3	**Deletion and return upon termination of customer relationship** Upon termination of processing of personal data by the Data Controller, data in accordance with the agreement with the Data Controller are: • Returned to the Data Controller, and/or • Deleted where it does not conflict with other legislation.	We have carried out enquiry with appropriate personnel of the data processor. On request We have been informed that the system design of the platform allows the data controller to retrieve all personal data either continuously or, at the latest, upon the conclusion of a campaign. We have observed that information is, by default, deleted 30 days after a campaign has concluded. Playable has formalized procedures for the deletion and return of data. We have inspected and confirmed that Playable has policies for data deletion and reporting. We have randomly inspected terminated customer agreements and observed that the customers have churned, and their licenses have been deactivated data are deleted.	No deviations were found.

Control Area E			
Control objectives *Procedures and controls are complied with to ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
E.1	**Storage of information is in accordance with the data controller's requirements** There are written procedures that require that personal data is only stored in accordance with the agreement with the data controller. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that formalized procedures are in place, which include requirements that personal data is stored solely in accordance with the agreement with the data controller. We have reviewed Playable's general security policy and data processor agreement procedure and observed that Playable has a procedure for accessing personal data based on principles of work-related necessity. We have observed that Playable has a procedure for encrypting information and that data is encrypted. We have observed that Playable has a procedure for the physical storage of personal data. We have observed that Playable has a procedure for storing personal data as long as there is a legal basis or legitimate reason. We have observed that the procedure has been updated in October 2024.	No deviations were found.
E.2	**Location of processing and storage of information** The data processing by the Data Processor, including storage, may only take place in the locations, countries or territories approved by the Data Controller.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that formalized procedures are in place, which include requirements that personal data is stored only at locations in accordance with the agreement with the data controller.	No deviations were found.

Control Area F			
Control objectives *Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
F.1	**Sub-data processing agreement and instructions** There are written procedures that contain requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected Playable's procedure for data processor agreements and observed that Playable informs customers about the use of sub-processors We have inspected notifications regarding new sub-processors and observed that Playable provides information about changes Upon request, we have been informed that Playable uses three sub-processors and has entered into standard agreements, including the processing of personal data within the EU. Furthermore, we randomly inspected that one of the sub-processors has adhered to the EU-U.S. Data Privacy Framework. We have inspected that the procedures have been updated and approved during the declaration period.	No deviations were found.
F.2	**Approval of sub-processors** The Data Processor only uses sub-processors for the processing of personal data that has been specifically or generally approved by the Data Controller.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected the data protection policy, customer overview, and data processor agreements and observed that data controllers, upon entering into an agreement with Playable, have approved the specified sub-processors. We have observed that Playable has a procedure for contracting sub-processors. We have observed that Playable has conducted audits of processes and sub-processors.	No deviations were found.

Control Area F			
Control objectives *Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
F.3	**Changes in approved sub-processors** In the event of changes in the use of generally approved sub-processors, the data controller is informed in a timely manner in relation to being able to object and/or withdraw personal data from the data processor. In the event of changes in the use of specifically approved sub-processors, this is approved by the data controller.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there are formalized procedures for notifying the data controller of changes in the use of sub-processors. We have inspected documentation that the data controller has been notified of a change in the use of sub-processors in accordance with entered data processing agreements.	No deviations were found.
F.4	**The subprocessor's obligations** The Data Processor has imposed on the sub-processor the same data protection obligations as those provided for in the Data Processing Agreement or similar with the Data Controller.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that data processing agreements have been entered into with the sub-processors used. We have inspected sub-data processing agreements to ensure that they contain the same requirements and obligations as are stated in the data processing agreements between the data controllers and the data processor.	No deviations were found.
F.5	**Overview of sub-processors** The data processor has a list of approved sub-processors stating: • Name • CVR no. • Address • Description of the treatment	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the data processor has a comprehensive and updated overview of used and approved sub-processors. We have inspected that the overview contains at least the required information about the individual sub-processor.	No deviations were found.

Control Area F

Control objectives
Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.

No.	Control activity	Tests conducted by BDO	Test result
F.6	**Supervision of sub-processors** On the basis of an updated risk assessment of the individual sub-processor and the activity carried out by the sub-processor, the data processor conducts an ongoing follow-up of this at meetings, inspections, review of the audit statement or similar. The data controller is informed of the follow-up that has been carried out at the sub-processor.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected documentation that a risk assessment has been made of the individual sub-processor and the current processing activity of the sub-processor. We have inspected that the data processor has carried out supervision, including obtaining and reviewing the sub-data processor's auditor's statements, certifications and the like. We have inspected that the data processor's supervision of sub-processors has not given rise to any further action. We have inspected documentation that the data processor has informed the data controller of the follow-up carried out by the sub-data processor.	No deviations were found.

Control Area H

Control objectives
Procedures and controls are complied with to ensure that the data processor can assist the data controller with the disclosure, correction, deletion or restriction of information about the processing of personal data to the data subject.

No.	Control activity	Tests conducted by BDO	Test result
H.1	**Procedure for fulfilling the rights of data subjects** There are written procedures that require the data processor to assist the data controller in relation to the rights of the data subjects. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there are formalized procedures in place for the data processor's assistance of the data controller in relation to the rights of the data subjects. We have inspected that the procedures have been updated and approved.	No deviations were found.
H.2	**Technical measures for the fulfilment of data subjects' rights** The data processor has established procedures which, to the extent agreed, enable timely assistance to the data controller in relation to the disclosure, correction, deletion or restriction of, and information about the processing of, personal data to the data subject.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable has a procedure for assisting the data controller with regard to the rights of data subjects. On request, we have been informed that no request for assistance has been made in relation to the rights of the data subjects.	We have established that there has been no request for assistance in relation to the rights of the data subjects. We have therefore not been able to test the control for implementation and efficiency. No deviations were found.

Control Area I			
Control objectives *Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement entered into.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
I.1	**Notification of personal data breaches** There are written procedures that require the data processor to notify the data controllers in the event of a personal data breach. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a personal data breach. We have inspected that the procedure has been updated and approved during the declaration period.	No deviations were found.
I.2	**Identification of personal data breaches** The Data Processor has established the following controls for the identification of any personal data breaches: • Awareness among employees	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the data processor provides awareness training to employees in relation to the identification of any personal data breaches.	No deviations were found.
I.3	**Timely notification of personal data breaches** In the event of any personal data breaches, the Data Processor has notified the Data Controller without undue delay and no later than 72 hours after becoming aware that a personal data breach has occurred at the Data Processor or a sub-data processor.	We have carried out enquiry with appropriate personnel of the data processor. We have observed that Playable has a procedure for notifying breaches of personal data security. We have inspected the procedure for notifying breaches of personal data security and observed that breaches are notified no later than 72 hours after being made aware of them. Upon request, we have been informed that Playable has not identified any breaches of personal data security during the reporting period, and therefore the implementation and effectiveness of the procedure have not been tested.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the control for implementation and efficiency. No deviations were found.

Control Area I			
Control objectives *Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement entered into.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
		On request, we have been informed that no incidents have been identified that have led to personal data breaches during the declaration period.	
I.4	**Assistance to data controllers in the event of a personal data breach** The Data Processor has established procedures for assistance to the Data Controller in its notification to the Danish Data Protection Agency: • The nature of the personal data breach • Likely consequences of the personal data breach • Measures that have been taken or are proposed to be taken to deal with the personal data breach.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected the data protection policy and procedures for data processing agreements and observed that Playable has a procedure for assisting the data controller in relation to breaches of personal data security. We have observed that no incidents have been identified that have led to personal data breaches during the declaration period.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the control for implementation and efficiency. No deviations were found.

Control area J			
Control objectives *Procedures and controls are complied with that ensure information security and data protection are planned and implemented in the data processor's development and change process.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
J.1	**Change management and privacy-by-design** The Data Processor has established a procedure for development and change tasks that ensures compliance with the privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and requirements for approval before implementation.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that the data processor has established a procedure for development and modification tasks that ensures compliance with the privacy-by-design principles, and that all development and modification tasks follow a formalized process that ensures testing and requirements for approval before implementation. We have randomly inspected for implemented changes/development that compliance with the privacy-by-design principles has been ensured in the development/change tasks. We have also inspected that the tasks have followed the formalized process, and that tests have been carried out and that the changes/developments have been approved before implementation.	No deviations were found.
J.2	**Implementing change in the production environment** The data processor has established a procedure for implementing changes in the production environment that ensures separation of functions in the implementation process.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that there is a separation of functions so that developers cannot implement changes directly in the production environment.	No deviations were found.
J.3	**Separation of the development, test, and production environment** Development and testing are performed in development environments that are separate from production environments.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that development, testing and production environment are separate.	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 the Lead De-

Control area J			
Control objectives *Procedures and controls are complied with that ensure information security and data protection are planned and implemented in the data processor's development and change process.*			
No.	**Control activity**	**Tests conducted by BDO**	**Test result**
			veloper and Head of Development have access to deploy software changes from development environment into production environment. No further deviations were found.
J.4	**Access to source code** Source code is protected from unauthorized modification and deletion.	We have carried out enquiry with appropriate personnel of the data processor. We have inspected that only the data processor's developers have access to source code. We have inspected documentation that the source code is protected against unauthorized modification and deletion.	No deviations were found.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 288000 AARHUS C

www.bdo.dk

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, 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: 37.96.xxx.xxx
2025-01-24 12:13:29 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 37.96.xxx.xxx
2025-01-24 16:49:49 UTC

Marianne Sejr Pharsen
COO
Serienummer: 89535f13-0ab0-47cd-a825-75e2be02c00b
IP: 80.208.xxx.xxx
2025-01-26 08:18:22 UTC