Data Processing Agreement: Apperta - inidus

1. Contents

2. Definitions

The definitions of abbreviations and terms used in this document are detailed below.

ITEM	DEFINITION
Access	Actions that may result in: (i) the data being viewed or changed; (ii) operational aspects of IT systems to changed; or (iii) security settings of IT systems to viewed or changed.
Agreement [1]	DiADeM Service Use Agreement: Main
Agreement [2]	IT Services Agreement

Agreement [3]	DiADeM Service Use Agreement: Apperta-User
Agreement [4]	Data Processing Agreement: Apperta-inidus
Agreement [5]	Data Processing Agreement: User- inidus
Apperta	The Apperta Foundation C.I.C., Company registered in England and Wales registration number: 09483987, Registered address: 10 Queen Street Place, London, EC4R 1BE
Apperta Data and Systems	(i) any DataDC for which Apperta is the Data Controller; and (ii) all Apperta IT Systems
Apperta IT Systems	All IT systems that Apperta controls to undertake Processing of DataDD where: (i) processing includes management of the data processing; (ii) the IT systems are under the control of Apperta; and (iii) IT Systems include DiADeM Web Service Tools.
Apperta Personnel	Those persons directly employed by Apperta; and subcontractors and agents working under Apperta's direct control
Assessor	This is a User role, where the User is registered to carrying out the DiADeM assessment on patients.
Breach of Personal Data	A breach of personal data means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
CDR	Clinical Data Repository
CESG	Communications-Electronics Security Group. This is is now part of National Cyber Security Centre (https://www.ncsc.gov.uk/). The UK government's National Technical Authority for Information Assurance (CESG), advises organisations on how to protect their information and information systems against today's threats.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, as defined by Article 4 of the GDPR.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, as defined by Article 4 of the GDPR.
Data Protection Officer (DPO)	Information Governance Role, defined under Article 39 of the GDPR.
Data Subject	A natural person who is the owner of the Personal Data

DataDC	Data that is controlled by the Data Controller
DataDD	Any data that is stored on the DiADeM Service.
DiADeM	Diagnosing Advanced Dementia Mandate, a dementia diagnostic tool to support the diagnosis of people living with advanced dementia in care home settings. It is designed for use on people living with advanced dementia within a care home who do not have a formal diagnosis. In these cases a referral to memory services may not be feasible or desirable, and is likely to be distressing for the individual.
DiADeM app	The app that the Assessor downloads to their remote device which they use to undertake the DiADeM Assessment.
DiADeM Assessment	A tool that has been developed in 2015 by the Yorkshire & Humber Dementia and Older Peoples Mental Health Clinical Network (YH DOPMH CN) with input from a range of stakeholders including experts in the field of Dementia from across the health spectrum and in particular from Dr Graeme Finlayson and Dr Subha Thiyagesh who shared their existing protocols. The application has support from the Alzheimer's Society and its use for diagnosing Dementia in the care home setting has been recommended by Professor Alistair Burns the National Clinical Director for Dementia and Older People's Mental Health.
DiADeM Assessment Report	the report generated as an outcome of a completed DiADeM Assessment. This report is in a pdf format and the Assessor sends this to their selected Recipient.
DiADeM Authentication Service	The Authentication Service holds User information for the purposes of managing permitted access and sharing of information held by the Diadem Service.
DiADeM CDR Service	The CDR Service is used to hold patient data (includes sensitive data). It comprises the CDR server and demographics server.
DiADeM Service	The Diadem Service are the full suite of services through which the DiADeM is delivered to Users.
DiADeM web portal	The web portal through which Users gain access to the Diadem Service.
DiADeM Web Service Tools	The tools provided through which the User accesses the Diadem Service.
DPcdr	The Data Processor of the DiADeM CDR Service

DPIA	Data Protection Impact Assessment (refer to Article 35 of GDPR, and https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)
ITServices	All IT services that inidus provides to support the DiADeM Service
ehrID	The unique internal identifier for a single patient, created by the DiADeM CDR Service
GDPR	General Data Protection Regulations (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en)
Information Commissioner's Office (ICO)	refer to https://ico.org.uk/
inidus	inidus Limited, Company registered in England and Wales registration number: 10733421, Registered address: The Oakley, Kidderminster Road, Droitwich, WR9 9AY
inidus Data and Systems	(i) any DataDC; and (ii) all inidus IT Systems
inidus IT Systems	All IT systems that inidus controls to undertake Data Processing of DataDD, including management of the data processing, where the systems are under the control of inidus
inidus Personnel	Those persons directly employed by inidus; and subcontractors and agents working under inidus' direct control
non-Clinical Auditor	This is a User role, where the User is able to obtain reports based on the full data held by the DiADeM Service. All reports are processed such that they contain NO patient Personal Data
Person identifiable Data (PID)	This is the same as Personal Data
Personal Data	Any data relating to an identified or identifiable natural person, as defined by Article 4 of the GDPR, that is stored on the inidus platform
PurposeDP	For inidus to discharge inidus' obligations as Data Processor of the DiADeM CDR Server
Privacy Impact Assessment (PIA)	Privacy Impact Assessment. This is defined under the Data Protection Act (refer to https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf). Note that, under the GDPR, the PIA is replaced by the DPIA.
Recipient	This is a User role, where the User is a clinician responsible for the long term care of the patient, or works for a clinician who is responsible for the patient's long term care. A Recipient is a person to whom an Assessor is able to send a DiADeM Assessment Report.
Retention Period	The time period that Personal Data is held by the DiADeM Service, after which point it being deleted.

Sensitive Data	Referred to as a special category of Personal Data within Article 9 of GDPR, and includes health data
Third Party	All persons or organisations who are not party to the agreement. Where one of the party is "inidus", then Third party excludes all inidus Personnel
User	The person who has registered on the DiADeM system to use the Diadem Service
User Role	The role that the User is registered on the Diadem Service. A User may register under one or more of the following roles types: (1) Assessor (2) Recipient (3) non-clinical Auditor
Working Hours	Working hours are defined as 9 a.m. to 5 p.m. on Monday to Friday, excluding bank holidays

3. Parties in the agreement

1. **Apperta**

2. **inidus**

4. Appointment

1. Under this agreement, **Apperta**, in its capacity as **Data Controller** of **DataDC** held by the **DiADeM Authentication Service**, appoints **inidus** to act as **Data Processor.**

5. Subject Matter

1. The subject matter of this agreement is **DataDC** for which **Apperta** is the **Data Controller**.

2. The agreements listed on the table below are relevant to this **Agreement [4]**.

3. This **Agreement [4]** is subordinate to the IT Services Agreement (**Agreement [2]**).

Title of Agreement	Abbreviation	Parties of agreement

IT Services Agreement	**Agreement [2]**	Apperta, inidus
Data Processing Agreement: Apperta-inidus	**Agreement [4]**	Apperta, inidus

6. Duration and Closure of Agreement

6.1. Duration

1. The duration of this agreement is indefinite

6.2. Notice

1. Notice may be served by the superior agreement **Agreement [2]** issuing a “Notice of IT Services termination”.

2. Where Notice is served, then the notice period of this **Agreement [4]** is the same as **Agreement [2]**.

6.3. End of Contract Provisions

1. The end of contract provisions are as detailed in the superior **Agreement [2]**.

7. Nature and Purpose of the Processing

1. The purpose of the processing covered under this agreement is to support the operation of the **DiADeM Service**. This is a clinical tool to assess moderate onset dementia.

2. Details of the **DiADeM Service** are provided at the link.

8. Type of Personal Data and categories of Data Subject

1. The type of **Personal Data** covered within this agreement are:

    a. Name of **Data Subject**;
    b. Contact details of **Data Subject**;
    c. Organisation for whom the **Data Subject** is undertaking work concerning **DiADeM**; and
    d. Organisations with which the **Data Subject** is associated within a professional capacity, and which has interests in the **Data Subject**'s work concerning **DiADeM.**

2. The categories of **Data Subject**s are Users who register to use the **DiADeM Service**.

3. The categories of **Data Subject** covered under this agreement does NOT include patients.

9. Obligations and Rights of the Data Controller

9.1. Compliance with applicable laws and regulations

1. **Apperta** shall act in full accordance with its duties as **Data Controller**.

2. **Apperta** shall handle **DataDC** in strict compliance with the prevailing data protection legislation applicable to the UK.

3. Nothing in this agreement relieves the **Data Controller** of its own direct responsibilities and liabilities under **GDPR**.

9.2. Documented Instructions

9.2.1. General Instructions

1. **Apperta** agrees to issue complete and comprehensive instructions to **inidus** concerning the processing of data covered under this agreement, where the instructions are fully compliant with **GDPR** Article 29.

2. **inidus** is required in all cases to confirm that the authentication key is genuine, prior to executing any instruction that **inidus** receives.

9.2.2. Specific instruction to be issued by Apperta

1. **Apperta** will issue API instructions in the form of an AQL query instruction to inidus, to obtain the following data from the **DiADeM Authentication Service**:

    a. For all **User**s who are **Data Controllers** of data held by the **DiADeM Service**:
        i. The Name of the **User**
        ii. The contact details of the **User**
        iii. The **ehrIDs** for all data for which the **User** is the **Data Controller**

2. **Apperta** will deliver the information obtained by this search, to **inidus**, and will instruct **inidus** to use the information for the sole **PurposeDP**.

3. **Apperta** will deliver updates to **inidus** of the information obtained by this search that are timely and prompt, whenever there are any changes to the **DataDD** corresponding to the data types detailed in clause (1)**.**

4. Where and only if the situation pertains where the **User** is no longer a **Data Controller** of any **Data Subject**'s **Data**, Apperta will instruct **inidus** to delete data supplied to **inidus**.

9.3. Security of Access Credentials

1. **Apperta** will keep secure all access credentials to the **inidus** services.

2. Where there is a breach or suspected breach of the security of these credentials by **Apperta** or a party providing services to **Apperta**, then **Apperta** will, at the earliest opportunity, change or reset the access credentials.

3. **Apperta** will inspect system logs to check that there has been no breach of Personal Data. **Apperta** will request support of **inidus** if there are more detailed investigations required.

9.4. Breach of Personal Data

In all cases where there is a **Breach** or suspected **Breach of Personal Data** for which **Apperta** acts as **Data Controller**, **Apperta** will**:**

1. Record:

    a. All **Breaches of Personal Data** even if they do not need to be reported;
    b. The facts relating to the breach, its effects and remedial action taken.

2. Assess the likely risk to the rights and freedoms of the **Data Subject**s as a result of a breach as detailed under Section IV of the Article 29 **GDPR** Working Party;

3. Notify the **ICO** of the **Breach** (in their capacity as the lead supervisory authority) without undue delay but not later than 72 hours of becoming aware of the **Breach** where the risk assessment indicates a potential risk to the rights and freedoms of the **Data Subject**;

4. Where the risk assessment indicates a potential HIGH risk to the rights and freedoms of the **Data Subject** inform the **Data Subject** of the risk, without undue delay.

5. Investigate whether the **Breach** was a result of human error or a systematic issue and establish how a recurrence can be prevented.

10. Obligations and Rights of the Data Processor

10.1. Compliance with applicable laws and regulations

1. **inidus** shall act in full accordance with its duties as **Data Processor.**

2. **inidus** shall handle **DataDC** in strict compliance with the prevailing data protection legislation applicable to the UK.

3. Nothing in this agreement relieves the **Data Controller** of its own direct responsibilities and liabilities under the prevailing data protection legislation applicable to the UK.

10.2. Data Processing actions

10.2.1. Documented Instructions

1. As a **Data Processor, inidus** will act only on the documented instructions that **inidus** receives from the **Data Controller** (in compliance with **GDPR** Article 28.3(a)).

2. **inidus** requires that instructions that it receives from the DiADeM Web Tools will use the secure API that **inidus** has provided to **Apperta** for use with the **DiADeM Service**.

3. **inidus** requires that **inidus** receives all instructions accompanied by a valid authentication key.

10.2.2. Instruction to carry out the processing

1. **inidus** will not process data except on instructions from the **Data Controller** in compliance with **GDPR** Article 29.

10.2.3. Execution of Instructions

1. **Inidus** will always validate the instruction prior to execution by:
    a. confirm that the authentication key is genuine.

10.2.4. Lawful processing of data

1. **inidus** will only act on the lawful instructions it receives from the **Data Controller** for the processing of **DataDC**.

2. Where **inidus** is required to undertake processing by direction of a legal authority or legal requirement, then **inidus** will inform the **Data Controller** prior to undertaking the processing, unless the law prohibits **inidus** communicating this information to the **Data Controller**.

3. In cases where **inidus** has concerns on the lawful nature of instruction that it receives, **inidus** will:

    a. Not execute the **Data Processing** instruction; and
    b. Inform the **Data Controller** of **inidus**' concerns and any actions that **inidus** may have taken as a result.

10.2.5. Instructions for Erasure when data is held on Backups

1. **Inidus** has a backup policy that requires that there are system backups maintained at all times for reasons of operational resilience. The backups are retained for a period of up to three months as specified in the **inidus Security Policy** and **inidus Standing Operating Procedures**, after which the data of the backup is deleted. It is not possible to erase the **Personal Data** from the backups without causing undue cost.

2. Where **inidus** receives an instruction for the permanent erasure of **Personal Data**, **inidus** will:

    a. Erase the **Personal Data** from the Operational System of the DiADeM Service
    b. Record which backups hold the **Personal Data**
    c. Update the record as each backup expires with the associated deletion of the **Personal Data** from that backup.

3. In situations where **inidus** requires to use a backup that holds data due for erasure, inidus will ensure that the necessary **Personal Data** is erased prior to any data from the backup being released to **DiADeM Service Users**.

10.3. Appointment of DPO

1. **inidus** will appoint a **DPO** with the responsibility for managing compliance of **inidus'** data processing activities covered under this agreement, with applicable laws and regulations.

10.4. Service Performance

1. **inidus** aims to offer the **DiADeM Authentication Service** with an uptime of 99% (excluding scheduled maintenance) in any calendar month.

2. Where **inidus** fails to meet this uptime, **inidus** will waive all charges for that calendar month period.

3. Scheduled maintenance will occur between 0200 and 0400 daily

10.5. Duty of Confidentiality

1. **inidus** will ensure that **inidus Personnel** who undertake any **Data Processing** activities on **DataDC** held on the **DiADeM Authentication Service** or who have access to the **inidus IT Systems** are aware that they are subject to a duty of Confidentiality.

2. **inidus** will ensure this duty of Confidentiality is enshrined through a binding agreement between **inidus** and the **inidus Personnel**, prior to **inidus** permitting the **inidus Personnel** to have access to **DataDC**.

10.6. Security

1. **inidus** will operate according to the **inidus** Security Policy and Standard Operating Procedures that are compliant with the prevalent legislative data regulations concerning security of **Personal Data** and Article 32 of the **GDPR**.

2. **inidus** will deliver the appropriate level of security by implementing technical and organisational measures

3. **inidus** will determine the appropriate level of security by undertaking risk assessment (as defined within **inidus'** Security Policy and Standard Operating Procedures), where the assessment will include accidental or lawful destruction, loss alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

4. **inidus** will maintain the following security measures:

    a. Hosting of the **DiADeM Authentication Service** at a secure data centre that is **CESG** approved and ISO 27001 certified;

b. Encryption of all **Personal Data** held by **inidus** systems that sit outside the secure data centre;
c. Encryption of all **Data** in transit, outside the secure data centre;
d. Undertaking regular vulnerability and penetration testing on processing systems under **inidus'** control and implement mitigations for all vulnerabilities detected;
e. Logging of access and usage; and
f. Monitoring and Audit of technical and organisational systems and measures.

10.7. Control of Access: inidus Personnel

10.7.1. DataDC

1. **inidus** will restrict the purpose for which **inidus Personnel Access DataDC** to a limited number of prescribed operations:

    a. Provision of support to the **Data Controller**;
    b. Maintenance; or
    c. Where required to do so by a Court or other body with statutory authority.

2. **inidus** has no right or need to **Access** the **DataDC** for any other purposes.

3. **inidus** will comply with the following principles for **Access**ing **DataDC**:

    a. All **Access** is avoided whenever this is practical;
    b. All **Access** is authorised by the **Data Controller** in advance;
    c. All **access** is authorised by a designated **inidus** manager;
    d. Only authorised persons are permitted to have access; and
    e. All access by **inidus Personnel** who know the person to whom the **DataDC** belongs is avoided.

4. **inidus** will maintain records of:

    a. **inidus Personnel** who have the ability to **Access** the **DataDC**, listing the purposes for which they are authorised to exercise this capability;
    b. All **Access** that has been made, the reasons for **Access** and authorisations for **Access,** where access by **inidus Personnel** has been made; and
    c. Actions taken where the **Access** was not authorised.

10.7.2. All inidus IT Systems

1. **inidus** will restrict **Access** of **inidus IT Systems** exclusively to **inidus Personnel**

2. **inidus** will comply with the following principles for permitting **Access** by **inidus Personnel** to **inidus IT Systems**:

    a. All **Access** is avoided whenever this is practical;
    b. All **access** is authorised by a designated **inidus** manager; and
    c. Only authorised persons are permitted to have **Access**.

2. **inidus** will maintain records of all permissions granted for **Access** to all **inidus IT Systems**. The records will include:

    a. Name,
    b. Organisation
    c. Contact details; and
    d. Purpose for access**.**

3. **inidus** will maintain records of actions taken where the **Access** was not authorised.

4. **inidus** will regularly review **Access** permissions and purpose for **Access** and make necessary changes to permissions commensurate with the purpose for which the **Access** is granted.

10.7.3. Approval for Access

inidus will exercise the following control of **Access** rights of **inidus Personnel** to **Inidus Data and Systems**:

1. Approval:
    a. **inidus Personnel** will require approval by the **inidus**' **Data Protection Officer (DPO)** for any increase in rights of **Access**.

2. Review:
    a. **inidus** will regularly review the activities by **inidus personnel** who have **Access**.
    b. The review will include the purpose for which the **inidus Personnel** are authorised to exercise **Access**.
    c. **inidus** will make changes to permitted **Access** rights as appropriate according to the operational needs of the **inidus Personnel**.

10.7.4. Exceptional Access to DataDC

1. There are rare circumstances where the diagnosis and correction of system problems may require **inidus Personnel** to **Access** the **DataDC** in circumstances where it is not possible or practical to seek the consent of the customers concerned. In these cases, **inidus** will permit **inidus Personnel** to **Access** the **DataDC** without prior customer consent providing:

    a. the **inidus** Security Officer authorises approval prior to access;
    b. The **inidus** Security Officer notifies **inidus** Senior Management and the **DPO** at the earliest opportunity; and
    c. **inidus** fully informs the **Data Controller** as soon as possible of the **Access**.

10.7.5. Unauthorised Access

inidus will take the following actions if there is unauthorised **Access** by **inidus Personnel** to **inidus Data and Systems**:

1. Compliance with the conditions outlined in the section entitled “Breach of Personal Data” within this agreement.

2. Where there is any intentional **Access**:
    a. **inidus** will summarily dismiss the **inidus Personnel**.
    b. **Inidus** will consider further action that includes prosecution and notification to any relevant professional body for possible disciplinary action.

3. Where there is any unintentional **Access:**
    a. The **inidus Personnel** are required to report the incident to the **inidus DPO** at the earliest opportunity.
    b. The **inidus DPO** will carry out an investigation to determine if the circumstance of the unintentional access justifies disciplinary action.

10.8. Control of Access to DataDC: Data Controller

1. **inidus** shall provide the capability for the **Data Controller** to have full **Access** and control of the **DataDC** via a secure API interface**.**

2. **Inidus** will store **DataDC** held on the **DiADeM Authentication Service** in an open format.

3. **Inidus** will enable the **Data Controller** to export part or all of the **DataDC** in a commonly used, machine-readable and an open standard format and to delete it from the **DiADeM Authentication Service** at anytime, without hindrance from **inidus**.

10.9. Control of Access to inidus Data and Systems: Third parties

1. **inidus** will not allow any **Third Parties** to **Access DataDC** unless authorised by the **Data Controller.**

2. Where the **Data Controller** authorises **Access**, **inidus** will treat the person whom the **Data Controller** has authorised as if they were the **Data Controller** in relation to the data they have been authorised to **Access** and the **Data Controller** will be responsible for their actions.

3. **inidus** will not allow any **Third Parties** to **Access** any **inidus IT System.**

10.10. Appointment of sub-processors

1. **inidus** will appoint a sub-processor to provide the cloud infrastructure that will hold the **DataDC**.

2. The Sub-processor will:

    a. Provide hosting of the **DiADeM Authentication Service** at a secure data centre that is **CESG** approved and ISO 27001 certified;
    b. Enable Encryption of all **DataDC** in transit, outside the secure data centre; and
    c. Hold the data within the UK.

3. **inidus** will not engage another sub-processor without prior specific or general written authorisation of the **Data Controller**. **inidus** will provide a reasonable length of time for the **Data Controller** to provide objections to **inidus**.

10.11. Data Subject's rights

1. **inidus** will assist the **Data Controller** meet its obligations to **Data Subject**s under Chapter III of the **GDPR** “Rights of the **Data Subject**” by:

    a. Providing the technical capability for the **Data Controller** to query, modify or part delete the **DataDC** held on the **DiADeM Authentication Service**;
    b. Undertaking operations on behalf of the **Data Controller** that may include the querying, modification or part deletion of **DataDC**; and
    c. Responding to the **Data Controller**’s request in a timely manner, with the presumption that the **Data Controller** has made the request to **inidus** as early as is reasonable**.**

10.12. Assisting the Data Controller in meeting **GDPR** obligations

1. **inidus** will assist the **Data Controller** in meetings its **GDPR** obligations in relation to the:

    a. Investigation if there is a suspected breach or loss of Personal Data
    b. Security of processing;
    c. Notification of personal data breaches to the supervisory authority;
    d. Communication of a personal **Data Breach** to the **Data Subject**;
    e. Data protection impact assessments (DPIA); and
    f. Consultation with the supervisory authority where the DPIA indicates there is an unmitigated high risk to the processing.

2. **inidus’** assistance will take into account the nature of the processing being undertaken by **inidus** and the information available to **inidus**.

3. **inidus** will on request, cooperate with supervisory authorities including the ICO.

4. The **Data Controller** agrees to reimburse **inidus** reasonable costs that may be incurred by **inidus** to provide the required support.

10.13. Records of Processing Activities

1. **Inidus** will keep records of all processing activities relevant to the processing of **DataDC** (in compliance with Article 30.2). This will include all data processing instructions.

10.14. Audits and Inspections

1. **inidus** will make available to the **Data Controller** all information that is necessary to demonstrate that inidus is compliant with the Data Processor Obligations of Article 28 of the **GDPR** with regard to its processing of **DataDC** and which are stipulated within this agreement.

2. **inidus** will allow for and contribute to audits and inspections, conducted by the **Data Controller** or another auditor mandated by the **Data Controller**.

3. Where the auditor has been mandated by the **Data Controller**, then **inidus** will require that the auditor signs the **inidus** Non-Disclosure Agreement prior to **inidus** granting access to the auditor.

4. **inidus** will inform the **Data Controller** at the earliest opportunity if **inidus** considers that it has received a data processing instruction from the **Data Controller** that infringes the **GDPR** or related data protection law.

10.15. Breach of Personal Data

In all cases where there is a **Breach** or suspected **Breach of Personal Data** for which **inidus** acts as **Data Processor**, **inidus** will**:**

1. Notify the **Data Controller** without undue delay, after becoming aware of a **Breach of Personal Data**.

2. Record:

    a. All **Breaches of Personal Data**; and
    b. The facts relating to the **Breach of Personal Data**, its effects and remedial action taken.

3. Investigate whether the **Breach** was a result of human error or a systematic issue and establish how a recurrence can be prevented.

10.16. Rights to applications owned by Data Controller

1. **inidus** will NOT place any claims of ownership under this contract on any applications that the **Data Controller** builds that use the **DiADeM Authentication Service**. The **Data Controller** is free to run these applications elsewhere.

10.17. Assistance to the Data Controller to recover lost data

1. In situations where the **Data Controller** has accidentally lost data through its processing activities, **inidus** will apply all reasonable endeavours to recover the **DataDC**.

2. **inidus** will not hold responsibility for any loss of **DataDC**.

10.18. Backup

1. **inidus** will store the **DataDC** on fault tolerant systems making **DataDC** loss caused by failure of the **DiADeM Authentication Service** an unlikely event.

2. **inidus** will make daily backups of the **DataDC** with incremental snapshots recorded at a minimum of hourly intervals.

3. In the event of **DataDC** loss resulting from a **DiADeM Authentication Service** failure, **inidus** will restore the **DataDC** to the point of the most recent backup within four **Working Hours.**

11. General Provisions

11.1. Indemnification

1. **Apperta** agrees to hold harmless and indemnify **inidus**, and its, affiliates, officers, agents, employees, advertisers, licensors, suppliers or partners (collectively "**inidus** and Partners") from and against any third party claim arising from or in any way related to (a) **Apperta**'s breach of the Terms, (b) **Apperta's** use of the **inidus** Services, or (c) **Apperta's** violation of applicable laws, rules or regulations in connection with the **inidus** Services, including any liability or expense arising from all claims, losses, damages (actual and consequential), suits, judgments, litigation costs and legal fees, of every kind and nature.

2. In such a case, **inidus** will provide **Apperta** with written notice of such claim, suit or action, offer conduct of the claim to **Apperta** and provide reasonable assistance to **Apperta** (at **Apperta's** expense) to enable **Apperta** to defend such claims.

11.2. Other Content

1. The **inidus** Services may include hyperlinks to other websites or content or resources or email content. **Inidus** may have no control over any websites or resources which are provided by companies or persons other than inidus .

2. **Apperta** acknowledges and agrees that **inidus** is not responsible for the availability of any such external sites or resources, and does not endorse any advertising, products or other materials on or available from such websites or resources.

3. **Apperta** acknowledges and agrees that **inidus** is not liable for any loss or damage which may be incurred by **Apperta** or **Apperta's** End Users as a result of the availability of those external sites or resources, or as a result of any reliance placed by you on the completeness, accuracy or existence of any advertising, products or other materials on, or available from, such websites or resources.

11.3. Governing Law

1. This agreement shall be governed by the laws of England and Wales.

11.4. Force Majeure

1. In no event shall the **inidus** be responsible or liable for any failure or delay in the performance of its obligations hereunder arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, strikes, work stoppages, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, and interruptions, loss or malfunctions of utilities, or communications; it being understood that the **inidus** shall use reasonable efforts which are consistent with accepted practices within IT Services sector to resume performance as soon as.