Data Protection Policy

Change History Record

Approval process is done online on the platform.

Issue/Issuer	Description of Change	Completer	Date of Issue
1.0 - Alliantist	Introduction of Document	ISMS Creator	
1.0.1	Changes accordingly Ydeal's ISMS	DPO	2019/10/10
1.0.2	Changes accordingly Ydeal's ISMS	ISMS Board	2019/10/10
1.1.0	Approved	CEO	2019/10/17
1.1.1	Minor changes	ISMS Board	2020/04/14
1.1.2	Approved	CEO	2020/04/14
1.2.0	Major changes	DPO	2020/05/14
1.2.1	Review/Minor changes	CISO	2020/05/14
1.2.2	Review	TISO	2020/05/14
1.2.3	Review for document specifications	DPO	2020/05/22
1.2.4	Minor Changes	DPO	2020/08/07
1.2.5	Approved	CEO	2020/08/20

Purpose

The purpose of this document is to demonstrate the management board's commitment to the protection of personal data.

Policy Overview

The Board of ISMS of Ydeal, located at Rua dos Correios, 135. Souto, Santa Maria da Feira 4520-709 operates primarily in the business of IT healthcare solutions.

We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and information-related assets relevant to meet the purpose and goals of Ydeal. This includes the handling of personal data or “Personally Identifiable Information” (PII).

Furthermore, Ydeal Management Board is committed to ensuring compliance with the European Union General Data Protection Regulation (GDPR EU) and Law 58/2019 from 8 of August 2019 and any other data protection legislation or regulation relevant to our business operations.

In complying with the above-mentioned legislation and regulation, the organisation makes commitments to implement policies and processes related to that compliance and to make staff and relevant third parties aware of their responsibilities when handling personal data.

More detailed policies and processes thus support this policy, including our Information Security Policy. A GDPR EU compliance workspace is also maintained in line with the Comissão Nacional de Protecção de Dados (CNPD), the Portuguese Data Protection Authority recommendations. These are located and managed within the ISMS.online platform.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Scope

All employees and relevant interested parties associated with the organisation’s handling of personal data have to comply with this policy. Appropriate training and materials to support it are available.

Definitions

The key definitions of terms used within or referred to by this policy are based upon those in the GDPR EU or other recognised documentation and are contained in Annex A.

Organisational Responsibilities

Our Data Protection Officer has overall responsibility for the day-to-day implementation of this policy. Ydeal Management Board ensures that the Data Protection Officer is treated according to the Article 38 and 39 of the GDPR.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Specific Responsibilities:

Chief Information Security Officer (CISO)	• Assumes full accountability for the information controlled and processed by the organisation including PII • Is the face and figurehead of the organisation to Interested Parties. Holds a significant position in the organisation (C Level or one below), thus giving confidence to those parties that the organisation takes data protection and information security seriously.
Data Protection Officer	• Keeping the board updated about data protection responsibilities, risks and issues • Reviewing all data protection procedures and policies on a regular basis • Arranging data protection training and advice for all staff members and those included in this policy • Answering questions on data protection from staff, board members and other stakeholders • Responding to individuals such as clients and employees who wish to know which data is being held on them by Ydeal • Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing • Approving data protection statements attached to emails and other marketing copy • Addressing data protection queries from clients, target audiences or media outlets • Complying with other legislation and regulation relevant to data protection in marketing activities
Technical Information Security Officer (TISO)	• Ensure that information security risks have been identified and assessed, taking account of any special requirements for personal data. • Supporting and advising other responsible managers and individuals in regard to information security requirements, policies & controls.
	• Ensure all systems, services, software and equipment meet acceptable security standards • Checking and scanning security hardware and software regularly to ensure it is functioning properly • Researching third-party services, such as cloud services the company is considering using to store or process data

IT Manager	• Ensure that software is developed in compliance with company security policies. • Ensure that all IT members work in compliance with company security policies.

Staff data protection training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided on a regular basis and when specific trigger events occur e.g. threats or incidents affecting all or part of the organisation, its supply chain or other Interested Parties that might impact the organisation financially or reputationally.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of this training is compulsory and where appropriate will be evidenced (e.g., by task completion in the ISMS.online platform).

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation and is required under GDPR EU. Whenever personal data is being collected we will document and provide a Privacy Notice in line with the requirements of Article 13 of the GDPR EU.

A template privacy notice is located within the ISMS.online platform.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing (described further below) and this will be specifically documented in the ISMS.online platform. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all GDPR EU principles of processing personal data.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Sensitive personal data

In case of processing sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure the health and safety at work). Any such consent will need to identify clearly what the relevant data is, why it is being processed and to whom it will be disclosed.

Fair, lawful and transparent processing

We must process personal data fairly, lawfully and in a transparent manner in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening, including profiling.

Under GDPR EU, processing of personal data is lawful only if at least one of the following apply:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps

c) at the request of the data subject prior to entering into a contract;

d) processing is necessary for compliance with a legal obligation to which the controller is subject;

e) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

g) authority vested in the controller;

h) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,

i) except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The processing of all personal data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Accuracy and relevance, i.e., purpose limitation and data minimisation.

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate, you should record the fact that the accuracy of the information is in dispute and inform the Data Protection Officer.

Data Portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.

A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Protection Officer will be responsible for conducting Privacy Impact Assessments (PIA) and ensuring that all IT and other relevant projects commence with a privacy plan. ISMS.online provides a PIA framework that is used for managing the process and documenting the approach.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data security

We must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Data Protection Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

The organisation has a documented “Information Security Policy” and a set of subordinate security policies and controls relating to our management of data and information security, including pseudonymisation, encryption and other measures accordingly GDPR EU. These are held within the ISMS.online platform.

Data retention

We must not retain personal data for longer than is necessary. What is “necessary” will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Data retention schedules will be maintained showing the minimum and maximum periods of retention for each data set. These are held within the ISMS.online platform in Personal Data Inventory & Records Processing Tracker.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Integrity and confidentiality

We must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Staff Responsibilities

All individual staff members are responsible for playing their part in maintaining the confidentiality, integrity and availability of personal data in compliance with the GDPR EU, Law 58/2019 from 8 of August 2019 and organisational policies, standards and procedures.

You must familiarise yourself with the requirements contained in this policy and any other relevant security policy and comply with any requirements relating to the proper handling and security of personal data.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Handling others' personal data

You must familiarise yourself with the organisational responsibilities detailed above and ensure that you comply with these whenever you are handling personal data. Special care and attention must be given when handling sensitive personal data.

Processing data in accordance with the individual's rights

You must abide by any request from an individual not to use their personal data for direct marketing purposes. Notify the Data Protection Officer about any such request if it falls outside of the normal processes or you have any reason to be unsure about the appropriate practice.

Contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity to ensure compliance with all relevant data protection and other legislation.

Reporting Personal Data breaches

All members of staff have an obligation to report actual or potential data protection weaknesses, events and incidents where compliance may be breached. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the CNPD of any compliance failures that are material either in their own right or as part of a pattern of failures

The reporting of such weaknesses, events and incidents will be managed through our Information Security Incident Management processes.

Monitoring

Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. ISMS board will monitor it regularly to make sure it is being adhered to.

Subject Access Requests

Responding as a Data Controller

Where Ydeal acts as a data controller it follows “CNPD” oriented practices towards Subject Access Requests (SAR), summarised below with all SAR being managed on the SAR Track.

Key principles - Ydeal will comply with all SAR within one month of receipt and will not charge for managing a request unless the effort required is excessive or unfounded. The process is as follows:

Incoming requests that are not business as usual enquiries* are recorded as To Do's on the SAR Track from whatever source they arrive.

A validation is carried out to ensure the request is bona fide asking for enough evidence of the requester's identity to confirm it. It is then categorised accordingly on the Track so it can be treated appropriately e.g. a third party or child focused request.

If required, clarification takes place with the requester to clarify the request.

If the request requires excessive effort or is unfounded the organisation may choose to charge the requester a reasonable fee based on the administrative cost of providing the information or choose not to respond*.

If appropriate an acknowledgement will be made to the requester that their request is being processed where the internal search and processing will take place with the appropriately validated scope. Assuming it is available the information is gathered ready for internal approval on what should be released.

An internal approval process will take place where the relevant internal authority [DPO] will approve the information proposed for release.

No changes to the actual records are to be made at this stage, it is simply: a) an assessment of whether any information found needs to be redacted or removed in relation to other people's information b) whether any of the information found in the search is subject to exemption** and c) that it is easily understood by the requester.

Release of the approved information will take place when it is put in the release status of the Track and then recorded with a copy or link to the released communication.

The SAR will then be marked as appropriately resolved and maintained on the Track. The request can be reopened and follow a similar process above, or when appropriately archived, or deleted in accordance with the data retention policies.

*If the enquiry is business as usual e.g. updating or changing customer details as part of normal business then it can be dealt with using the normal processes. General routine work can continue during a SAR with records being updated as required.

**Data subject to exemption includes data being processed for purposes such as crime detection & prevention. More information can be found on the CNPD website.

Responding as a Data Processor

Where Ydeal is a data processor and receives a SAR it will record that on the SAR Track as a To Do. Unless otherwise stated in the agreement with the data controller it will then forward that request onto the data controller to manage in accordance with its own SAR processes. Where appropriate a communication will be made back to the requester explaining it has been forwarded onto the data controller for its information, but they have to approach the data controller directly. We will send the contact details for doing that at the same time. The communication will be resolved in the SAR Track item as 'sent to data controller' for audit purposes.

How we communicate this to potential requesters

The request should be sent to dpo@ydeal.pt;

There is no fee unless the request is excessive or unfounded then explains the options for payment if required;

The information that the requester will need to provide to confirm their identity will be sent by email.

The 30-day period for responding to the request which starts immediately on receipt unless a payment is due then it commences once the payment has been received (except the right to object Art. 21.º, where we will act immediately upon your request).

We give details of a point of contact for any questions.

*When choosing not to respond to the SAR

CNPD guidance will be followed when choosing not to respond and this will include an explanation of why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Annex A – Key Definitions

Data Subject	**Personal Data** means any information relating to an identified or identifiable natural person (**Data Subject**).*[source GDPR EU]*
Personal Data	**Personal Data** is any information relating to an identified or identifiable natural person (**Data Subject**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier

	or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *[source GDPR EU]*
Sensitive Data or Special categories of personal data	**Special Categories of Personal data** (**Sensitive Data**) is any information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*[source GDPR EU]*
Controller	**Controller** means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. *[source GDPR EU]*
Processor	**Processor** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller. *[source GDPR EU]*
Recipient	**Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. *[source GDPR EU]*
Processing	**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. *[source GDPR EU]*
Profiling	**Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. *[source GDPR EU]*

Pseudonymisation	**Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. *[source GDPR EU]*
Consent	**Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. *[source GDPR EU]*
Personal Data Breach	**Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. *[source GDPR EU]*