Genuine Happiness, Serviços Digitais Unipessoal Lda
DATA RETENTION POLICY
28 April 2021

1. **Introduction**

This Policy sets out the obligations of **Genuine Happiness, Serviços Digitais Unipessoal Lda** (the "**Company**") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("**GDPR**").

This policy does not form part of any employment contract and we may amend it at any time.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed;

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR); or

e) When the personal data has to be erased to comply with a legal obligation.

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

2. **Aims and Objectives**

The aims of this Policy are (i) to set out limits for the retention of personal data; (ii) to ensure that those limits, as well as further data subject rights to erasure, are complied with; (iii) to ensure that the Company complies fully with its obligations and safeguard the rights of data subjects under the GDPR; and (iv) to improve the speed and efficiency of managing data.

3. **Scope**

This Policy applies to all personal data held by the Company which is stored in the following ways and in the following locations:

a) Third-party servers, operated by Amazon Web Services, and located in the United Kingdom, the United States, and the European Union;

b) Computers permanently located in the Company's premises at Vau, 2510-662, Portugal;

c) Laptop computers and other mobile devices provided by the Company to its employees;

d) Computers and mobile devices owned by employees, agents, and contractors;

e) Physical records stored in Vau, 2510-662, Portugal;

4. **Data Disposal**

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

4.1.1 Personal data stored electronically (including any and all backups thereof) shall be permanently deleted; and

4.1.2 Personal data stored in hardcopy form shall be shredded and securely disposed of.

5. **Data Retention**

5.1.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

5.1.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

5.1.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Company's legal basis for collecting, holding, and processing that data; and

e) The category or categories of data subject to whom the data relates.

5.1.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

5.1.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Legal contracts	Legal compliance	2 years	6 years for contracts that are not executed by deed and 12 years for contracts that are executed by deed.	
Audited financial statements, tax returns and assessments and banking records	Legal compliance	2 years	6 years	
Records establishing client's identity for money laundering purposes	Legal compliance	2 years	5 years	
Records establishing client's identity	Performance of business activities	2 years	5 years	
Job applications and interview records of unsuccessful candidates	Performance of business activities	2 years	A short period, perhaps 6 months after notifying unsuccessful candidates (or longer, if there is a clearly communicated policy to keep candidates CVs for future reference).	Application forms should give applicants the opportunity to object to their details being retained.

Personnel and training records	Performance of business activities	2 years	While employment continues and up to six years after employment ceases.	
Written particulars of employment, contracts of employment, and changes to terms and conditions	Performance of business activities	2 years	While employment continues and up to six years after employment ceases.	
Working time opt-out forms	Performance of business activities	2 years	Two years from the date on which they were entered into.	
Annual leave records	Performance of business activities	2 years	Six years or possibly longer if leave can be carried over from year to year.	
Payroll and wage records for companies	**Performance of business activities**	2 years	Six years from the financial year-end in which payments were made.	
PAYE records	**Performance of business activities**	2 years	Not less than three years after the end of the tax year to which they relate.	
Maternity / paternity records	**Performance of business activities**	2 years	Three years after the end of the tax year in which the maternity pay period ends	
Sickness records required for the purposes of Statutory Sick Pay	**Performance of business activities**	2 years	Three years after the end of the tax year in which payments are made.	
Any reportable accident, death or injury in connection with work	**Performance of business activities**	2 years	For at least three years from the date the report was made.	
Consents for the processing of personal and sensitive data.	**Legal compliance**	2 years	For as long as the data is being processed and up to 6 years afterwards	

Recycle bins	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Downloads	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Email inbox	**Performance of business activities**	2 years	For 5 years from email's date.	
Deleted emails	**Performance of business activities**	2 years	For 5 years from email's date.	
Personal network drive	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Local drives and files	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Google drives	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Dropbox	**Performance of business activities**	2 years	For 5 years from document's last modified date.	
Call recordings	**Performance of business activities**	2 years	For 5 years from date of call.	
Prospect data	**Performance of business activities**	2 years	For 5 years from date of first contact.	
Live chat history	**Performance of business activities**	2 years	For 5 years from date of chat.	
Metrics data	**Performance of business activities**	2 years	For 5 years from date of data acquisition.	
CRM data	**Performance of business activities**	2 years	For 5 years from date of first contact.	

Tender documents	**Performance of business activities**	2 years	For 5 years from date of submission.	
Board minutes	**Performance of business activities**	2 years	For 5 years from date of meeting.	
Business expenses	**Performance of business activities**	2 years	For 5 years from date of expense.	
Non-audited financial statements	**Performance of business activities**	2 years	For 5 years from date of statement.	
Customer complaints	**Performance of business activities**	2 years	For 5 years from date of complaint.	
Data protection requests	**Performance of business activities**	2 years	For 5 years from date of request.	
Health & Safety records	**Performance of business activities**	2 years	For 5 years from date of record.	
Insurance policies	**Performance of business activities**	2 years	For 5 years from date of policy.	
Insurance claims	**Performance of business activities**	2 years	For 5 years from date of claim.	
CCTV recordings	**Performance of business activities**	2 years	For 5 years from date of recording.	

6. **Roles and Responsibilities**

6.1.1 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Privacy-related policies (including, but not limited to, its Privacy Policy), and with the GDPR and other applicable data protection legislation.

6.1.2 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company**.**

6.1.3 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

7. **Implementation of Policy**

This Policy shall be deemed effective as of 22 March 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Miguel Morin
Position:	Chief Executive Officer
Date:	28 April 2021
Due for Review by:	27 April 2022
Signature: