<<insert company name>>
Data Protection Policy

1. Introduction

This Policy sets out the [illegible] Company name>>, a company registered in <<insert cou[illegible]under number <<insert company registration number>>, w[illegible] is at <<insert address>> ("the Company") regarding data[illegible]ghts of <<insert type(s) of data subject, e.g. staff, custom[illegible]etc.>> in respect of their personal data under UK Data Protec[illegible]below).

This Policy sets the Com[illegible]arding the collection, processing, transfer, storage, and disp[illegible]The procedures and principles set out herein must be follow[illegible]Company, its employees, agents, contractors, or other parties[illegible]e Company.

2. Definitions

"consent" [illegible]onsent of the data subject which [illegible]eely given, specific, informed, and [illegible]s indication of the data subject's [illegible]hich they (by a statement or by a [illegible]tive action) signify their agreement [illegible]ssing of personal data relating to

"data controller" [illegible]erson or organisation which, alone [illegible]n others, determines the purposes [illegible]f the processing of personal data. [illegible]oses of this Policy, the Company [illegible] controller of all personal data [illegible]<insert type(s) of data subject, e.g. [illegible]mers, business contacts etc.>> [illegible]usiness;

"data processor" [illegible]person or organisation which [illegible]ersonal data on behalf of a data

"Data Protection Legislat[illegible] [illegible]applicable data protection and [illegible] including, but not limited to, the [illegible] law version of the General Data [illegible]Regulation ((EU) 2016/679) (the [illegible]), as it forms part of the law of [illegible]d Wales, Scotland, and Northern [illegible]rtue of section 3 of the European [illegible]ndrawal) Act 2018, the Data [illegible]Act 2018, the Privacy and [illegible]ommunications Regulations 2003 [illegible], and any successor legislation;

"data subject"	iving, identified, or identifiable bout whom the Company holds a;
"EEA"	European Economic Area, all EU Member States, Iceland, n, and Norway;
"personal data"	information relating to a data can be identified, directly or particular by reference to an uch as a name, identification ation data, an online identifier, or re factors specific to the physical, , genetic, mental, economic, ocial identity of that data subject;
"personal data breach"	each of security leading to the or unlawful destruction, loss, unauthorised disclosure of, or ersonal data transmitted, stored, processed;
"processing"	operation or set of operations on personal data or sets of a, whether or not by automated ch as collection, recording, structuring, storage, adaptation n, retrieval, consultation, use, y transmission, dissemination or making available, alignment or restriction, erasure or
"pseudonymisation"	rocessing of personal data in such at the personal data can no longer to a specific data subject without dditional information, provided that nal information is kept separately ct to technical and organisational ensure that the personal data is d to an identified or identifiable n; and
"special category person	nal data revealing racial or ethnic itical opinions, religious or beliefs, trade union membership, xual life, sexual orientation, genetic data.

3. **Data Protection Officer &**

3.1 The Company's Da <<insert name of data protection officer>>, <<insert he Data Protection Officer is responsible for adm for developing and implementing any applicable rela those referred to in this Policy), procedures, and/or

3.2 All <<insert appli managers, department heads, supervisors etc.>> uring that all employees, agents, contractors, or othe half of the Company comply with this Policy and, whe ement such practices, processes, controls, and trai ly necessary to ensure such compliance.

3.3 Any questions relat mpany's collection, processing, or holding of persona Protection Legislation should be referred to the Data

4. **The Data Protection Princ**

The Data Protection Legisl ng principles with which any party handling personal data mus ata must be:

4.1 processed lawfully, ent manner in relation to the data subject;

4.2 collected for spec imate purposes and not further processed in a ma le with those purposes. Further processing for arch blic interest, scientific or historical research purposes shall not be considered to be incompatible with th

4.3 adequate, relevant is necessary in relation to the purposes for which

4.4 accurate and, wher date. Every reasonable step must be taken to ensure s inaccurate, having regard to the purposes for which , or rectified without delay;

4.5 kept in a form which data subjects for no longer than is necessary for the p rsonal data is processed. Personal data may be store ofar as the personal data will be processed solely f the public interest, scientific or historical research p rposes, subject to implementation of the appropriate te nal measures required by the Data Protection Legislati d the rights and freedoms of the data subject;

4.6 processed in a man riate security of the personal data, including protection unlawful processing and against accidental loss, d using appropriate technical or organisational meas

5. **The Rights of Data Subje**

The Data Protection Legis wing key rights applicable to data subjects:

5.1 The right to be infor

5.2 the right of access;

5.3 the right to rectificat

5.4 the right to erasure to be forgotten');

5.5 the right to restrict p

5.6 the right to data por

5.7 the right to object; a

5.8 rights with respect t aking and profiling.

6. **Lawful, Fair, and Transpa**

6.1 The Data Protecti o ensure that personal data is processed lawfully, y, without adversely affecting the rights of the data su ocessing of personal data shall be lawful if at least one

a) the data sub o the processing of their personal data for one es;

b) the processi erformance of a contract to which the data sub er to take steps at the request of the data sub a contract;

c) the processi npliance with a legal obligation to which the da

d) the processi ect the vital interests of the data subject or of

e) the processi erformance of a task carried out in the public in of official authority vested in the data controll

f) the processi urposes of the legitimate interests pursued by a third party, except where such interests are mental rights and freedoms of the data subject on of personal data, in particular where the da

6.2 **[**If the personal data ategory personal data (also known as 'sensitive perso f the following conditions must be met:

a) the data sub licit consent to the processing of such data fo urposes (unless the law prohibits them from d

b) the process he purpose of carrying out the obligations a ghts of the data controller or of the data subject ment, social security, and social protection la thorised by law or a collective agreement p ovides for appropriate safeguards for the funda sts of the data subject);

c) the processi ect the vital interests of the data subject or son where the data subject is physically or g consent;

d) the data con ssociation, or other non-profit body with a politi ous, or trade union aim, and the processing ourse of its legitimate activities, provided tha solely to the members or former members of who have regular contact with it in

connection … that the personal data is not disclosed ou… e consent of the data subjects;

e) the processi… ta which is manifestly made public by the data s…

f) the process… the conduct of legal claims or whenever co… dicial capacity;

g) the processi… stantial public interest reasons, on the basis of … ortionate to the aim pursued, shall respect the e… ta protection, and shall provide for suitable and… safeguard the fundamental rights and interests…

h) the process… he purposes of preventative or occupational… ssment of the working capacity of an employee… for the provision of health or social care or treat… nt of health or social care systems or services … ursuant to a contract with a health professional… ns and safeguards referred to in Article 9(3) o…

i) the processi… lic interest reasons in the area of public healt… ing against serious cross-border threats to h… tandards of quality and safety of health care … s or medical devices, on the basis of law which… d specific measures to safeguard the rights an… subject (in particular, professional secrecy); or

j) the process… rchiving purposes in the public interest, sc… esearch purposes, or statistical purposes in… le 89(1) of the UK GDPR (as supplemente… ata Protection Act 2018) based on law which s… o the aim pursued, respect the essence of … ion, and provide for suitable and specific me… he fundamental rights and the interests of t…

7. **Consent**

If consent is relied upon as… ecting, holding, and/or processing personal data, the following…

7.1 Consent is a clea… subject that they agree to the processing of their … ear indication may take the form of a statement or a p… re-ticked boxes, or inactivity are unlikely to amount t…

7.2 Where consent is … which includes other matters, the section dealing wit… clearly separate from such other matters.

7.3 Data subjects are f… at any time and it must be made easy for them to do… draws consent, their request must be honoured promp…

7.4 If personal data is t… erent purpose that is incompatible with the purpose o… hat personal data was originally

collected that was … a subject when they first provided their consent, cons… e or purposes may need to be obtained from the d…

7.5 **[**If special category … ssed, the Company shall normally rely on a lawful bas… nsent. If explicit consent is relied upon, the data sub… e issued with a suitable privacy notice in order to ca…

7.6 In all cases where … as the lawful basis for collecting, holding, and/or proc… cords must be kept of all consents obtained in order to… y can demonstrate its compliance with consent require…

8. Specified, Explicit, and L…

8.1 The Company colle… personal data set out in <<insert location(s)>>. This i…

a) personal dat… data subjects**[**.**] OR [**; and**]**

b) **[**personal da… rties.**]**

8.2 The Company only … and holds personal data for the specific purposes … tion(s)>> (or for other purposes expressly permitted … egislation).

8.3 Data subjects must … times of the purpose or purposes for which the Comp… data. Please refer to Part 15 for more information on … nformed.

9. Adequate, Relevant, and … g

9.1 The Company will c… personal data for and to the extent necessary for the s… oses of which data subjects have been informed (or w… r Part 8, above, and as set out in <<insert location(s)>…

9.2 Employees, agents … parties working on behalf of the Company may col… to the extent required for the performance of the… in accordance with this Policy. Excessive personal … ed.

9.3 Employees, agents … parties working on behalf of the Company may proc… when the performance of their job duties requires it. P… e Company cannot be processed for any unrelated re…

10. Accuracy of Data and Ke…

10.1 The Company shal… al data collected, processed, and held by it is kept ac… This includes, but is not limited to, the rectification of p… est of a data subject, as set out in Part 17, below.

10.2 The accuracy of pe… ecked when it is collected and at **[**regular**] OR [**<<ins… thereafter. If any personal data is found to be inacc… reasonable steps will be taken

without delay to am s appropriate.

11. **Data Retention**

11.1 The Company shall for any longer than is necessary in light of the purpose that personal data was originally collected, held, and

11.2 When personal data l reasonable steps will be taken to erase or otherwise y.

11.3 For full details of ach to data retention, including retention periods fo ypes held by the Company, please refer to our Data Re

12. **Secure Processing**

12.1 The Company sha sonal data collected, held, and processed is kept against unauthorised or unlawful processing and ag destruction, or damage. Further details of the techn easures which shall be taken are provided in the C ty Policy**]** **AND/OR [**IT Security Policy**]**.

12.2 All technical and or aken to protect personal data shall be regularly reviewe re their ongoing effectiveness and the continued secur

12.3 Data security must s by protecting the confidentiality, integrity, and availa as follows:

a) only those w ccess and use personal data and who are auth ess and use it;

b) personal da and suitable for the purpose or purposes for d, and processed; and

c) authorised u le to access the personal data as required for r purposes.

13. **Accountability and Reco**

13.1 The Data Protectio r administering this Policy and for developing and im ble related policies, procedures, and/or guidelines.

13.2 The Company sha esign approach at all times when collecting, holding, nal data. Data Protection Impact Assessments shall cessing presents a significant risk to the rights and fre (please refer to Part 14 for further information).

13.3 All employees, age r parties working on behalf of the Company shall be g in data protection and privacy, addressing the rele Protection Legislation, this Policy, and all other applica

13.4 The Company's da e shall be regularly reviewed and evaluated by means ts.

13.5 The Company sha al records of all personal data collection, holding, a all incorporate the following:

a) the name ar y, its Data Protection Officer, and any applicab ers (including data processors and other data c sonal data is shared);

b) the purpose y collects, holds, and processes personal dat

c) the Compar es (including, but not limited to, consent, the ning such consent, and records of such conser and processing personal data;

d) details of t onal data collected, held, and processed b he categories of data subject to which that p

e) details of an ata to non-UK countries including all mechanis rds;

f) details of h will be retained by the Company (please refe Retention Policy);

g) details of pe ding location(s); and

h) detailed des al and organisational measures taken by the security of personal data.

14. **Data Protection Impact A y by Design**

14.1 In accordance with ples, the Company shall carry out Data Protection Imp y and all new projects and/or new uses of personal da e of new technologies and where the processing inv in a high risk to the rights and freedoms of data su

14.2 The principles of p d be followed at all times when collecting, holding, a data. The following factors should be taken into consid

a) the nature, s ose or purposes of the collection, holding, and

b) the state o ant technical and organisational measures to

c) the cost of i res; and

d) the risks po d to the Company, including their likelihood an

14.3 Data Protection Imp e overseen by the Data Protection Officer and shall ad

a) the type(s) o e collected, held, and processed;

b) the purpose(a is to be used;

c) the Compan

d) how persona

e) the parties (who are to be consulted;

f) the necessit… …he data processing with respect to the purpose… …ocessed;

g) risks posed …

h) risks posed … …mpany; and

i) proposed m… …handle identified risks.

15. **Keeping Data Subjects In…**

15.1 The Company shall… … set out in Part 15.2 to every data subject:

a) where perso… …ctly from data subjects, those data subjects will … …se at the time of collection; and

b) where perso… …m a third party, the relevant data subjects will … …se:

i) if the… …d to communicate with the data subje… …nication is made; or

ii) if the… …ansferred to another party, before that t…

iii) as so… …le and in any event not more than one m… …data is obtained.

15.2 The following inform… …n the form of a privacy notice:

a) details of the… … not limited to, contact details, and the names a… … applicable representatives and its Data Protect…

b) the purpose… …al data is being collected and will be processe… …sert location(s)>>) and the lawful basis justifyi… …ocessing;

c) where applic… …rests upon which the Company is justifying its … …g of the personal data;

d) where the p… …ned directly from the data subject, the categorie… …cted and processed;

e) where the p… …transferred to one or more third parties, deta…

f) where the p… …ansferred to a third party that is located outs… …of that transfer, including but not limited to the… …ee Part 25 of this Policy for further details);

g) details of ap… …eriods;

h) details of … …nts under the Data Protection Legislation;

i) details of th… …o withdraw their consent to the Company's p… …nal data at any time;

j) details of t… … to complain to the Information Commission…

k) where the p… …ned directly from the data subject, details abou… …nal data;

l) where appli… …gal or contractual requirement or obligation ne… …n and processing of the personal data and det… …s of failing to provide it; and

m) details of a… …making or profiling that will take place using … …ding information on how decisions will be ma… … of those decisions, and any consequenc…

16. **Data Subject Access**

16.1 Data subjects may … …uests ("SARs") at any time to find out more about the … … Company holds about them, what it is doing with that …

16.2 Employees wishing… …d do so using a Subject Access Request Form, sen… …mpany's Data Protection Officer at <<insert contact det…

16.3 Responses to SAR… …ade within one month of receipt, however, this may … …wo months if the SAR is complex and/or numerous re… …ch additional time is required, the data subject shall b…

16.4 All SARs received s… …Company's Data Protection Officer **[**and in accordance… …ta Subject Access Request Policy & Procedure**]**.

16.5 The Company does… …he handling of normal SARs. The Company reserves … …nable fees for additional copies of information that has… …o a data subject, and for requests that are manifestly … …, particularly where such requests are repetitive.

17. **Rectification of Personal …**

17.1 Data subjects have… …e Company to rectify any of their personal data that is… …e.

17.2 The Company shall… …a in question, and inform the data subject of that recti… …n of the data subject informing the Company of the iss… …tended by up to two months in the case of complex re… … time is required, the data subject shall be informed.

17.3 In the event that … …data has been disclosed to third parties, those partie… …y rectification that must be made to that personal data…

18. **Erasure of Personal Data…**

18.1 Data subjects have… …the Company erases the personal data it holds about t… …umstances:

a) it is no long mpany to hold that personal data with respect hich it was originally collected or processed;

b) the data su w their consent to the Company holding and l data;

c) the data sub pany holding and processing their personal dat ding legitimate interest to allow the Company to e Part 21 of this Policy for further details conc ;

d) the personal d unlawfully;

e) the persona sed in order for the Company to comply with on**[**;**]** **OR [**.**]**

f) **[**the persona nd processed for the purpose of providing inf s to a child.**]**

18.2 Unless the Compa unds to refuse to erase personal data, all requests f plied with, and the data subject informed of the era n of receipt of the data subject's request. The perio up to two months in the case of complex requests. I required, the data subject shall be informed.

18.3 In the event that an o be erased in response to a data subject's request h ird parties, those parties shall be informed of the impossible or would require disproportionate eff

19. **Restriction of Personal D**

19.1 Data subjects may y ceases processing the personal data it holds abou ect makes such a request, the Company shall reta ersonal data concerning that data subject (if any) that that the personal data in question is not processed fur

19.2 In the event that data has been disclosed to third parties, those part of the applicable restrictions on processing it (unles d require disproportionate effort to do so).

20. **[Data Portability**

20.1 The Company pro sing automated means. <<Insert details of automate

20.2 Where data subject nt to the Company to process their personal data in su ocessing is otherwise required for the performance of e Company and the data subject, data subjects have a Protection Legislation, to receive a copy of their pe e it for other purposes (namely transmitting it to oth

20.3 To facilitate the righ Company shall make available all applicable personal he following format**[**s**]**:

a) <<list format

b) <<add furthe

20.4 Where technically f a data subject, personal data shall be sent directly to th r.

20.5 All requests for co hall be complied with within one month of the data s iod can be extended by up to two months in the case requests. If such additional time is required, the data s **]**

21. **Objections to Personal D**

21.1 Data subjects hav o the Company processing their personal data base s, for direct marketing (including profiling), **[**and proc r historical research and statistics purposes**]**.

21.2 Where a data subje ny processing their personal data based on its legitim any shall cease such processing immediately, unless d that the Company's legitimate grounds for such p ata subject's interests, rights, and freedoms, or that th y for the conduct of legal claims.

21.3 Where a data subje ny processing their personal data for direct marketin any shall cease such processing promptly.

21.4 **[**Where a data subj any processing their personal data for scientific and/o nd statistics purposes, the data subject must, unde egislation, "demonstrate grounds relating to his or h The Company is not required to comply if the resea performance of a task carried out for reasons of public

22. **[Automated Processing, aking, and Profiling**

22.1 **[**The Company use mated decision-making processes as follows:

a) <<Insert outl decision-making>>.**]**

22.2 **[**The Company uses ng purposes as follows:

a) <<Insert outl tivities>>.**]**

22.3 The activities outli d described in detail in <<insert location(s)>>) are g er the Data Protection Legislation where the resulting similarly significant effect on data subjects unless one

a) the data sub cit consent;

b) the processi r

c) the process entry into, or performance of, a contract bet he data subject.

22.4 If special category processed in this manner, such processing can only he following applies:

a) the data sub cit consent; or

b) the processi ons of substantial public interest.

22.5 Where decisions a automated processing (including profiling), data subj ject, to challenge such decisions, request human inte r own point of view, and to obtain an explanation of Company. Data subjects must be explicitly informed o nt of contact.

22.6 In addition to the a must be provided to data subjects explaining the logi ion-making or profiling, and the significance and en f the decision or decisions.

22.7 When personal data automated processing, automated decision-making, or hall apply:

a) appropriate l procedures shall be used;

b) technical a sures shall be implemented to minimise the ccur, such measures must enable them to be e

c) all personal this manner shall be secured in order to prev s arising.**]**

23. **[Direct Marketing**

23.1 The Company is su nd regulations when marketing its **[**products**] AND/OR**

23.2 The prior consent c red for electronic direct marketing including email, tex ated telephone calls subject to the following limited exc

a) The Compa g text messages or emails to a customer pr mer's contact details have been obtained in the marketing relates to similar products or s er in question has been given the opportunity g when their details were first collected an mmunication from the Company.

23.3 The right to objec hall be explicitly offered to data subjects in a clear and must be kept separate from other information in ity.

23.4 If a data subject ob g, their request must be complied with promptly. A li al data may be retained in such circumstances to ensure that the data subject's marketing preferenc ed with.**]**

24. **Personal Data Collected,**

Full details of the personal d processed by the Company are located in <<insert locatio ata retention, please refer to the Company's Data Retention

25. **Transferring Personal Da e the UK**

25.1 The Company may ansfer ('transfer' includes making available remotely) ries outside of the UK. The Data Protection Legislati s in order to ensure that the level of protection given t mpromised.

25.2 Personal data may country outside the UK if one of the following applies

a) The UK has rming that the country in question ensures an ection (referred to as 'adequacy decisions' o . From 1 January 2021, transfers of personal EA countries will continue to be permitted. T e also in place to recognise pre-existing EU e UK.

b) Appropriate including binding corporate rules, standard co ed for use in the UK (this includes those adopte mission prior to 1 January 2021), an approved pproved certification mechanism.

c) The transfe med and explicit consent of the relevant data

d) The transfer he other reasons set out in the UK GDPR inclu of a contract between the data subject an blic interest reasons; for the establishme of legal claims; to protect the vital interests of the data subject is physically or legally incap r, in limited circumstances, for the Company's l

26. **Data Breach Notification**

26.1 All personal data b ed immediately to the Company's Data Protection Offi

26.2 If an employee, ag r party working on behalf of the Company becomes that a personal data breach has occurred, they mus igate it themselves. Any and all evidence relating to ch in question should be carefully retained.

26.3 If a personal data b reach is likely to result in a risk to the rights and fre s (e.g. financial loss, breach of confidentiality, disc amage, or other significant social or economic dama on Officer must ensure that the Information Commi med of the breach without delay, and in any event, w g become aware of it.

26.4 In the event that a p kely to result in a high risk (that is, a higher risk than th 26.3) to the rights and freedoms of data subjects, the must ensure that all affected data subjects are informe and without undue delay.

26.5 Data breach notifica llowing information:

a) The categori ber of data subjects concerned;

b) The categor umber of personal data records concerned;

c) The name a Company's data protection officer (or other cor formation can be obtained);

d) The likely co h;

e) Details of t proposed to be taken, by the Company t including, where appropriate, measures to erse effects.

27. **Implementation of Policy**

This Policy shall be deem ert date>>. No part of this Policy shall have retroactive effec ly to matters occurring on or after this date.

This Policy has been approved an

Name: <<insert

Position: <<insert

Date: <<insert

Due for Review by: <<insert

Signature: