UCSP

UNIVERSITY COMMERCIAL SERVICES PLYMOUTH

UCSP Ltd

Data Protection Policy

Author:	Terri Cormack
Reviewed By:	Emma Wainman
First Published:	May 2021
Next Review Date:	May 2022

Table of Contents

1. Introduction 4
2. General Data Protection Regulation (GDPR) 4
2.1 Personal Data 4
2.2 The GDPR Principles 4
3. Policy Statement 5
4. Purpose 6
5. Scope 6
6. Definitions 6
7. Objectives 7
8. The Information Commissioners Office (ICO) 9
9. Governance Procedures 9
9.1 Accountability & Compliance 9
10.1.1 Privacy by Design 10
10.1.2 Data Minimisation 10
10.1.3 Encryption 11
10.1.4 Restriction 11
10.1.5 Hard Copy Data 11
10.1.6 Information Audit 12
10.2. Legal Basis for Processing (Lawfulness) 12
10.2.1 Processing Special Category Data 13
10.2.2 Records of Processing Activities 14
10.3 Third Party Processors 14
10.4 Data Retention & Disposal 15
11. Data Protection Impact Assessment (DPIA) 15
12. Data Subject Rights Procedures 16
12.1 Consent & Right to be Informed 16
12.1.1 Consent Controls 17
12.1.2 Child's Consent 18
12.1.3 Alternatives to Consent 18
12.1.4 Information Provisions 18
12.2 Privacy Notice 19
12.3 Personal Data not obtained from the Data Subject 20
12.3.1 Employee Personal Data 21
12.4 The Right of Access 21
12.4.1 Subject Access Request 22

12.6 Rectification & Erasure 22
12.6.1 Correcting Inaccurate or Incomplete Data 22
12.6.2 The Right to Erasure 23
12.7 Objections 23
13 Oversight Procedures 24
13.1 Security and Breach Management 24
14 Transfers & Data Sharing 24
15 Training 25
16 Penalties 25

Data Protection Policy

1. Introduction

In May of 2018 the GDPR law came into effect and they fundamentally changed the way we treat personal data and the owners of the data. This policy is in place to ensure all staff (including temporary and contractors), visitors and students are aware of their responsibilities and outlines how UCSP Ltd complies with the core principles of GDPR in relation to UCSP Ltd's business. The policy sets out UCSP Ltd's ambitions and acts as a framework for the implementation programme.

2. General Data Protection Regulation (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and applies to all EU Member States from 25th May 2018. As a *'Regulation'* rather than a *'Directive'*, its rules apply to Member States, replacing their existing local data protection laws and repealing Directive 95/46C and its Member State implementing regulation.

As UCSP Ltd processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

2.1 Personal Data

Information protected under GDPR is known as 'personal data'

UCSP Ltd ensures that a high level of care is afforded to personal data falling within the GDRP's **'special categories'** *(previously sensitive personal data*), due to the assumption that this type of information could be used in a negative or discriminatory way and is of sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR requires that:
"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Exemption clauses applies."

2.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

> ***a)*** processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***
>
> ***b)*** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***
>
> ***c)*** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that organisations such as UCSP Ltd show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

3. Policy Statement

UCSP Ltd needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, students, customers, suppliers, clients and visitors and includes *(but is not limited to),* name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details and categorised personal data.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or statutory bodies. However, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), UK data protection laws and any other relevant data protection laws and codes of conduct *(herein collectively referred to as "the data protection laws").*

UCSP Ltd has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach where first we ensure that we need to collect the data, then assess changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

4. Purpose

The purpose of this policy is to ensure that UCSP Ltd meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individual's, best interest.
The data protection laws include provisions that promote accountability and governance and as such UCSP Ltd has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches, ensuring good practice across the institution and uphold the protection of personal data.

5. Scope

This applies to anyone who has access to personal data as part of their relationship with UCSP Ltd. This includes, but is not limited to, all staff, students and contractors within UCSP Ltd (e.g. permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with UCSP Ltd). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action, or in the case of non-employees e.g. sub-contractors, termination of contract may apply.

6. Definitions

Term	Definition
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
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 for the agreed purpose (s).
Cross Border Processing	The processing of personal data which: - - takes place in more than one Member State; or - which substantially affects or is likely to affect data subjects in more than one Member State
Data Controller	The Data Controller, UCSP Ltd, determines the purposes and means of the processing of personal data; where the purposes and means of such 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.
Data Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.
Data Protection Laws	Means for the purpose of this document, the collective description of the GDPR, Data Protection Act 2018 (*referred to as the Act*) and any other relevant data protection laws that UCSP Ltd complies with.
Data Subject	Is an individual who is the subject of personal data
GDPR	General Data Protection Regulation *(EU) (2016/679)*

Genetic Data	Is personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
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, 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.
Processing	Is 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.
Profiling	Is 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.
Recipient	Is 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.
Special Category Data	Special category data is personal data which the GDPR says is more sensitive, and so needs more protection e.g. medical data, criminal record etc.
Supervisory Authority	Is an independent public authority which is established by a Member State which is in the UK the ICO
Third Party	Is a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

7. Objectives

We are committed to ensuring that all personal data processed by and on behalf of UCSP Ltd is done so in accordance with the data protection laws and their principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

UCSP Ltd has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

UCSP Ltd will implement appropriate measures to ensure that:

- We protect the rights of individuals with regards to the processing of personal information.

- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.

- Every business practice, function and process carried out by the UCSP Ltd, is monitored for compliance with the data protection laws and its principles.

- Personal data is only processed where we have verified and met the lawfulness of processing requirements.

- We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Act 2018 Schedule 1 conditions.

- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.

- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and UCSP Ltd.

- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws.

- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary.

- We monitor the Information Commissioner's Office, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements.

- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.

- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance.

- We provide clear reporting lines and supervision with regards to data protection.

- We store and destroy all personal information, in accordance with our Data Retention and Disposal policy and schedule, which has been developed from the legal, regulatory and statutory requirements and suggested timeframes.

- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice.

- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements.

- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place.

8. The Information Commissioners Office (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislations they have oversight for include: -

- The Data Protection Act 1998 *(pre-25th May 2018)*
- General Data Protection Regulation *(post-25th May 2018)*
- Data Protection Act 2018
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

UCSP Ltd is registered with ICO and appear on the Data Protection Register as a controller and/or processer of personal information. Our Data Protection Registration Number is ZA053299.

9. Governance Procedures

9.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by UCSP Ltd, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to:-

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance.
- Provide data protection training for all employees.
- Identify key stakeholders to support the data protection compliance program.
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role.
- Identify, create and disseminate the reporting lines within the data protection governance structure.

The technical and organisational measures that UCSP Ltd has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

10.1.1 Privacy by Design

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

10.1.2 Data Minimisation

Under article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only necessary data is collected includes:

- Electronic collection *(i.e. forms, website, surveys etc.*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include *'optional'* fields, as optional denotes that it is not necessary to obtain.
- Physical collection *(i.e. face-to-face, telephone etc.*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected.
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor).* These state that only

relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.
- Forms, contact pages and any documents used to collect personal information are reviewed every 6 months to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing.

10.1.3 Encryption

We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format.

10.1.4 Restriction

Our *Privacy by Design* approach means that we use UCSP Ltd-wide restriction methods for all personal data activities. Restricting access is built into the foundation of UCSP Ltd's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

10.1.5 Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options. Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***Steps include:***

- In the first instance we always ask the initial data controller to send copies of any personal information records directly to the data subject.
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*).
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (*i.e. we do not use the postal system as this can be intercepted*).
- Recipients (*i.e. the data subject, third-party processer*) are re-verified and their identity and contact details checked.
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the data protection laws*), we destroy the hard copy data.

If for any reason a copy of the paper data must be retained by UCSP Ltd, it must be kept in secured lockable filing cabinet.

10.1.6 Information Audit

To enable UCSP Ltd to fully prepare for and comply with the data protection laws, we have initiated a company-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process. This exercise will help create and develop a Data Registry Schedule.

The audit will identify, categorise and record all personal information obtained, processed and shared by UCSP Ltd in our capacity as a controller/processor and has been compiled on a central register it will include: -

- What personal data we hold.
- Where it came from.
- Who we share it with.
- Legal basis for processing it.
- What format(s) it is in.
- Who is responsible for it?
- Disclosures and Transfers.

10.2. Legal Basis for Processing (Lawfulness)

As the core of all personal information processing activities undertaken by the UCSP Ltd, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information asset register and in our Privacy Notice and, where applicable, is provided to the data subject and the Information Commissioner's Office as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where:***

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in UCSP Ltd.

- Processing is necessary for the purposes of the legitimate interests pursued by UCSP Ltd or by a third party (*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 minor).*

10.2.1 Processing Special Category Data

Where UCSP Ltd processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where:

- The data subject has given explicit consent to the processing of the personal.

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.

- Processing relates to personal data which are manifestly made public by the data subject.

- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Processing is necessary for reasons of substantial public interest.

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

- Processing is necessary for reasons of public interest in the area of public health.

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act 2018 provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Where UCSP Ltd processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. ***Measures include:***

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Act 2018 Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing

- Documenting the Schedule 1 condition and Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*

- Having an appropriate policy document in place when the processing is carried out, specifying our: -

    - Procedures for securing compliance with the data protection laws principles.
    - Policies as regards the retention and erasure of personal data processed in reliance on the condition.
    - Retention periods and reason *(i.e. legal, statutory etc.).*
    - Procedures for reviewing and updating our policies in this area

Please refer to our Disposal & Retention Policy for further guidance and procedures.

10.2.2 Records of Processing Activities

As an organisation with less than 250 employees, UCSP Ltd are obliged to document activities that are:

a) Not occasional; or
b) Could result in a risk to the right and freedoms of individuals; or
c) Involve the processing of special categories of data or criminal conviction and offence data

10.3 Third Party Processors

UCSP Ltd utilise external processors for certain processing activities (where applicable). We use information audits to identify, categorise and record all personal data that is processed outside of UCSP Ltd, so that information, processing activity, processor, legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes (but is not limited to):***

- IT Systems & Services
- Legal Services
- Debt Collection Services
- Human Resources
- Payroll
- Hosting or Email Servers
- Credit Reference Agencies

We have strict due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain the relevant documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obliged under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

10.4 Data Retention & Disposal

UCSP Ltd has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the right and privacy of data subjects *(e.g. shredding, disposal of confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

Please refer to our ***Data Disposal & Retention Policy*** for full details on our retention, storage, periods and destruction processes.

11. Data Protection Impact Assessment (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by UCSP Ltd. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where UCSP Ltd must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale categories of data.
- Processing on a large scale of personal data relating to criminal convictions and offences.
- Systematic monitoring of a publically accessible area on a large scale (i.e. CCTV)
- Where processing operation is likely to result in a high risk to the rights and freedoms of an individual.
- Those involving the use of new technologies.
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects.

- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIA's enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either:

- Eliminated
- Reduced
- Accepted

12. Data Subject Rights Procedures

12.1 Consent & Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the UCSP Ltd and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws. The data protection law defines consent as; *'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'.*

Where processing is based on consent, UCSP Ltd have reviewed and revised all content mechanisms to ensure that:

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms.

- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes.

- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data.

- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand.

- Pre-ticked, opt-in boxes are **never** used.

- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service).*

- Along with UCSP Ltd, we also provide details of any other third party who will use or rely on the consent.

- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case.

- Consent withdrawal requests are processed immediately and without detriment.

- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent.

- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents.

- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified.

12.1.1 Consent Controls

UCSP Ltd maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

Consent to obtain and process personal data is obtained by UCSP Ltd through:

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic (i.e. via website form)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

12.1.2 Child's Consent

While the GDPR states that a child's age is defined as 16; the UK's Data Protection Act 2018 reduces this age to ***13 years***, as per Article 8(1) of the data protection laws advises that *'Member states may provide by law for a lower age for those purposes that such lower age is not below 13 years.'*

The data protection laws state that where processing is based on consent and the personal data relates to a child who is below the age of 13 years, such processing is only carried out by the UCSP Ltd where consent has been obtained by the holder of parental responsibility over the child.

UCSP Ltd have mechanisms in place to verify the age of any child prior to obtaining consent and review such consents annually for transferring from parental consent over to the child after age 13.

12.1.3 Alternatives to Consent

UCSP Ltd recognises that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor:

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use.

- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate.

- Where there is an imbalance in the relationship, i.e. with employees.

12.1.4 Information Provisions

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, students etc., written materials and/or electronic formats i.e. website forms, subscriptions, Email etc.)*, we provide the below information in all instances, **in the form of a privacy notice:**

- The identity and the contact details of the controller and, where applicable, of the controller's representative.

- The contact details of our data protection officer.

- The purpose(s) of the processing for which the personal information is intended.

- The legal basis for the processing.

- Where the processing is based on point (f) of Article 6(1) *'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party',* details of the legitimate interests.

- The recipients or categories of recipients of the personal data *(if applicable).*

- If applicable, the fact that UCSP Ltd intends to transfer the personal data to a third country or international organisation and the existence / absence of an adequacy decision by the Commission.

- Where UCSP Ltd intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards UCSP Ltd has put in place and the means by which to obtain a copy of them or where they have been made available.

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- The right to lodge a complaint with the Supervisory Authority.

- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and if the possible consequences of failure to provide such data.

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent are managed and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

12.2 Privacy Notice

UCSP Ltd defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal data *(or at the earliest possibility where that data is on obtained indirectly).*

Our Privacy Notice includes the Article 13 *(where collected directly from individual)* or 14 *(where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notices on our website and provide a copy of physical and digital formats upon request. The notice is the student, staff and third party facing policy that provides the legal information on how we handle, process and disclose personal information.
The notice is easily accessible, legible and jargon-free and is available in several formats, dependent on the method of data collection:-

- Via our website

- Linked to or written in full at the foot of Emails

- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Via SMS
- Printed media, adverts and financial promotions.
- Digital Products/Services
- On Mobile Apps
- Automated phone service

Where we rely on consent to obtain and process personal information, we ensure that it is:

- Displayed clearly and prominently.
- Asks individuals to positively opt-in.
- Gives them sufficient information to make an informed choice.
- Explains the different ways we will use their information.
- Provides a clear and simple way for them to indicate they agree to different types of processing.
- Includes a separate unticked opt-in box for direct marketing.

12.3 Personal Data not obtained from the Data Subject

Where UCSP Ltd obtains and/or processes personal data that has not been obtained directly from the data subject, UCSP Ltd ensures that the information disclosures contain in Article 14 are provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information disclosures in section Information Provisions, where personal data has not been obtained directly from a data subject, we also provide them with information about:

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources.

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where UCSP Ltd intends to further process any personal data for a purpose ***other*** than that for which it was originally intended, we communicate this intention to the data subject prior to doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if:-

- They already have it and we can evidence their prior receipt of the information.
- The provision of such information proves impossible and/or would involve a disproportionate effort.
- Obtaining or disclosure is expressly laid down by Union or Member State law to which UCSP Ltd is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

12.3.1 Employee Personal Data

Our HR procedures have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Terms and Conditions booklet which informs them of their rights under the data protection laws, how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

All employees have access to their personal data via Employee Self Service and have the ability to exercise their rights as a data subject.

12.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

12.4.1 Subject Access Request

Where a data subject asks us to confirm whether we hold and process data concerning him or her and requests access to such data; we provide them with:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed.
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer.
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a Supervisory Authority.
- Where personal data has not been collected by the UCSP Ltd from the data subject, any available information as to the source and provider.

Subject Access Requests (SAR) are passed to the **Data Protection Officer** as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

12.6 Rectification & Erasure

12.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by UCSP Ltd is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The **Data Protection Officer/Responsible Person** are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit

being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

12.6.2 The Right to Erasure

Also known as *'The Right to be Forgotten',* UCSP Ltd complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by UCSP Ltd is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Records Disposal & Retention Policy for exact procedures on erasing data and complying with the Article 17 requirements.

12.7 Objections

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. ***Individuals have the right to object to:***

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling).*

- Direct marketing *(including profiling).*

- Processing for purposes of scientific/historical research and statistics.

Where UCSP Ltd processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subject's objection will only be considered where it is on *'grounds relating to their particular situation'.* We reserve the right to continue processing such personal data where:-

- We can demonstrate compelling legitimate grounds for the processing, which overrides the interests, rights and freedoms of the individual.

- The processing is for the establishment, exercise or defence of legal claims.

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, UCSP Ltd will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

13 Oversight Procedures

13.1 Security and Breach Management

Alongside our *'Privacy by Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our ***Information Security Policies*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits (DPIA) to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, UCSP Ltd has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our ***Data Breach Policy*** for specific protocols.

14 Transfers & Data Sharing

UCSP Ltd takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

15 Training

Through our strong commitment and robust controls, leaders ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role through our Performance Development Review process and regular 1 to 1s.

16 Penalties

UCSP Ltd its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach and they could be subject to disciplinary sanctions in accordance with the UCSP Ltd's Disciplinary Policy & Procedure. ***We recognise that:***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.