**Clauses to Comply with the General Data Protection Regulation[[1]](#footnote-2) (“GDPR”) and any legislation implemented in the UK in connection with the GDPR and any replacement legislation coming into effect from time to time, together “Data Protection Legislation”, whenever a “Processor” stores or processes personal data for the University (“the Controller”), supplementary to the Processor’s contract with the University.**

***IF NOT OTHERWISE SET OUT IN THE CONTRACT THE FOLLOWING TABLE NEEDS TO BE COMPLETED:***

|  |  |
| --- | --- |
|  | ***Insert details in this column*** |
| Types of personal data | “Personal Data”[[2]](#footnote-3) |  |
| Special category data[[3]](#footnote-4) |  |
| Types of data subjects (e.g. staff, students) |  |
| Description of work (subject matter, nature and purpose of processing activities e.g. data storage)  |  |
| Duration of processing |  |

Note: If the Processor determines the purposes and means of processing, contrary to the terms of the following clauses, the Processor shall be considered to be a controller in respect of such processing[[4]](#footnote-5).

Processor Obligations – *see GDPR Article 28(3)(a) to (h)*

The Processor shall ensure that it and any sub-processor (to be engaged only with the Controller’s consent and on the same terms as below[[5]](#footnote-6)) identifies the Personal Data as above and –

(a) in processing[[6]](#footnote-7) the Personal Data:

(i) does so only on documented instructions from the Controller;

(ii) does not transfer the Personal Data to a third country[[7]](#footnote-8) or an international organisation[[8]](#footnote-9), unless the Controller so instructs, or the Processor is required to do so by law;

(iii) if the Processor is required by law to make such a transfer, the Processor shall inform the Controller of that legal requirement before transferring, unless the law prohibits such information being given on important grounds of public interest;

(b) ensures that persons authorised to process the Personal Data are bound by contractual confidentiality obligations which reflect the requirements of these clauses and the need to keep the Personal Data secure and confidential[[9]](#footnote-10);

(c) ensures appropriate technical and organisational measures are in place[[10]](#footnote-11) to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation and encryption of the Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident;

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

and in assessing the appropriate level of security account may be taken of adherence to an approved code of conduct[[11]](#footnote-12), and shall[[12]](#footnote-13) be taken of:

1. the state of the art, the costs of implementation and the nature, scope, context and purposes of processing[[13]](#footnote-14);
2. the risk of varying likelihood and severity for the rights and freedoms of natural persons)[[14]](#footnote-15);
3. the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data transmitted, stored or otherwise processed[[15]](#footnote-16);

(d) does not engage another processor (a sub-processor) unless the Controller in its absolute discretion gives a specific or general written authorisation; and where such consent is given, the Processor[[16]](#footnote-17):

(i) shall inform the Controller of any intended changes to a general written authorisation to add or replace processors, thereby giving the Controller the opportunity to object to such changes[[17]](#footnote-18);

1. shall impose the same data protection contractual obligations as set out in these clauses[[18]](#footnote-19);

(iii) acknowledges that the Processor remains fully liable to the Controller for the performance of the sub-processor[[19]](#footnote-20);

(e) assists the Controller by appropriate technical and organisational measures, so far as possible, to respond to requests for exercising the data subject's rights under Data Protection Legislation, including Chapter III of the GDPR[[20]](#footnote-21);

(f) assists the Controller[[21]](#footnote-22) with:

(i) their joint obligation to ensure that appropriate technical and organisational security measures are in place[[22]](#footnote-23);

(ii) notifying any Personal Data breach to the supervisory authority (the UK ICO) and to the data subject[[23]](#footnote-24);

(iii) data protection impact assessments and consulting the supervisory authority where an assessment indicates the processing involves unmitigated high risk[[24]](#footnote-25);

(g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Data Protection Law requires storage of the Personal Data[[25]](#footnote-26); and

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this clause and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; and immediately informs the Controller if, in its opinion, an instruction infringes Data Protection Legislation[[26]](#footnote-27).

1. EU 2016/679 (“GDPR”) Article (“Art”) 28

 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> [↑](#footnote-ref-2)
2. any information relating to an identified or identifiable natural person, 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 (Art 4(1)) [↑](#footnote-ref-3)
3. 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 (Art 9(1)) [↑](#footnote-ref-4)
4. Art 28(10) [↑](#footnote-ref-5)
5. Art 28(4) [↑](#footnote-ref-6)
6. Art 28(3)(a) [↑](#footnote-ref-7)
7. a country outside the European Union (Recital 101) [↑](#footnote-ref-8)
8. an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries (Art 4(24)) [↑](#footnote-ref-9)
9. Art 28(3)(b) [↑](#footnote-ref-10)
10. Art 28(3)(c) and Art 32 [↑](#footnote-ref-11)
11. Art 32(3) [↑](#footnote-ref-12)
12. Art 32(1) and (2) [↑](#footnote-ref-13)
13. Art 32(1) [↑](#footnote-ref-14)
14. Art 32(1) [↑](#footnote-ref-15)
15. Art 32(2) [↑](#footnote-ref-16)
16. Art 28(2) and Art(3)(d) [↑](#footnote-ref-17)
17. Art 28(2) [↑](#footnote-ref-18)
18. Art 28(4) [↑](#footnote-ref-19)
19. Art 28(4) [↑](#footnote-ref-20)
20. Art 28(3)(e) [↑](#footnote-ref-21)
21. Art 28(3)(f) [↑](#footnote-ref-22)
22. Art 32 [↑](#footnote-ref-23)
23. Art 33 and 34 [↑](#footnote-ref-24)
24. Art 35 and 36 [↑](#footnote-ref-25)
25. Art 28(3)(g) [↑](#footnote-ref-26)
26. Art 28(3)(h) [↑](#footnote-ref-27)