Data Rights Policy

CONTENTS

CLAUSE

1. Purpose

1.1. The University of Law has adopted this Policy to address procedures for handling data subject requests and objections under the GDPR when we act as a data controller. The GDPR grants data subjects certain rights regarding their personal data including the right to:

i. Access their personal data under GDPR Article 15.

ii. Correct their personal data under GDPR Article 16.

iii. Erase their personal data under GDPR Article 17.

iv. Restrict personal data processing about them under GDPR Article 18.

v. Receive a copy of certain personal data or transfer that personal data to another data controller, also known as the data portability right, under GDPR Article 20.

vi. Object to personal data processing under GDPR Article 21.

vii. Not be subject to automated decision-making in certain circumstances under GDPR Article 2

1.2. The purpose of the Policy is to formalise procedures for:

(a) Confirming the identity of the data subject making a request and the identity of the third party making a request on a data subject's behalf.

(b) Recording and tracking data subject requests and responses, including all correspondence and internal documents related to requests.

(c) Identifying and locating relevant personal data.

(d) Determining whether a GDPR or other exemption exists that permits or requires us to refuse to fulfil the request.

(e) Handling data subject requests that involve several data subjects' personal data.

(f) Communicating with data subjects at reasonable intervals regarding the status of their request.

2. Scope

2.1. This Policy applies to all of The University of Law employees. The department responsible for handling these requests include the Data Protection Department.

2.2. The Legal Department is responsible for Oversight and Guidance.

2.3. The Information Technology (IT) department is responsible for processing the request where applicable.

2.4. The Human Resources department is responsible for ensuring all staff are aware of the policy and overseeing any disciplinary hearing due to non-adherence to the policy.

3. Definitions

i. **Data controller** means the natural or legal person that determines the purposes and means of processing personal data (The University of Law). This policy only applies when The University of Law acts as a data controller and not when the organization acts as a data processor as defined below.

ii. **Data subject** means the person about whom the data controller collects and processes personal data.

iii. **Data processor** means a natural or legal person that processes personal data (defined below) on behalf of a data controller such as The University of Law third-party vendors or affiliates, subsidiaries and related corporate entities providing services. The University of Law may act as a data processor in certain situations for affiliates, related corporate entities and third parties. However, this policy does not apply to The University of Law personal data processing activities as a data processor. If you have any questions about whether the University of Law is acting as a data controller or a data processor, please contact the DPO mailbox.

iv. **GDPR** means the EU General Data Protection Regulation (Regulation (EU) 2016/679).

v. **Joint controller** means two or more data controllers jointly determining the purposes and means of processing. The responsibilities of each joint data controller are set out in arrangement between them including their responsibilities in responding to data subject requests. If you have any questions about whether The University of Law acts as a joint controller and its responsibilities as a joint controller, please contact DPO Mailbox.

vi. **Personal data** means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified directly or indirectly by reference to an identifier, such as a name, identification number or online identifier.

vii. **Processing** means any operation or set of operations performed on personal data, whether or not by automated means such as collection, use, storage, dissemination and destruction.

viii. **Profiling** means any form of automated processing of personal data to evaluate aspects about a data subject. This includes, for example, predicating aspects about that individual's performance at work, economic situation, health, personal preferences, interests, behaviour or location.

4. Data Subject Request Submission Format

4.1. The University of Law require all data subjects seeking to exercise their GDPR rights to use our standard request forms. These standard request forms ask data subjects for specific information necessary to process and respond to their request. Data subjects must submit the form applicable to their type of request which is available from the DPO and can be accessed at University Policies https://www.law.ac.uk/about/policies/ . If a data subject cannot access or fill out the online form they must submit their requests in writing to the DPO.

OR

All data subjects seeking to exercise their rights under the GDPR must submit their requests in writing to the DPO mailbox DPO@law.ac.uk

4.2. If you receive an oral data subject request, direct the data subject to submit the request by using The University of Law standard request forms which is available at https://www.law.ac.uk/about/policies/

OR

If you receive an oral data subject request, direct the data subject to submit the request to the DPO Mailbox DPO@law.ac.uk

5. Tracking Data Subject Requests

5.1. All data subject requests received must be forwarded to the following e-mail address DPO@law.ac.uk.

5.2. The DPO must continuously track the following regarding data subject requests

(a) Date of data subject request.

(b) Data subject name.

(c) Requester name (if applicable).

(d) Assigned employee(s) that will handle data subject request.

(e) Request status (new, in progress, completed).

(f) Request format.

(g) Method(s) of identification.

(h) Data subject ID.

(i) Request type.

(j) Request details.

(k) Interim response date(s) (if applicable).

(l) Final response date.

(m) Final disposition.

6. Acknowledging Receipt of Data Subject Requests

6.1. DPO must maintain all correspondence and documentation related to data subject requests in the Data Subject Request Folder.

6.2. DPO must advise the data subject in writing that The University of Law received the request and that the data subject should expect to receive a response within one month.

7. Involve Relevant Departments

7.1. DPO must provide the data subject request to the relevant department, with a subject line entitled “Data Subject Request immediately after receiving the data subject request. This helps ensure that the appropriate departments begin to locate and identify relevant personal data and address any legal issues related to the data subject request.

7.2. The legal department, must assign an individual (s) to handle the data subject request (This is normally the DPO).

8. Proof of Data Subject’s Identity

8.1. We must verify a data subject’s identity before we can respond to a data subject request. If a data subject makes a request electronically by using The University of Law email account with a username or other unique identifier, additional documents to prove the data subject’s identity is not necessary.

8.2. Data subjects that cannot verify their identity online through a username or unique identifier must provide identification that clearly shows their name, date of birth and current address. We accept a photocopy or a scanned image of the following as proof of identity: passport or photo identification such as a driver’s licence, national identification number card, birth or adoption certification etc. If data subjects changed their name they must provide relevant documents evidencing the change.

8.3. We must store all identification documentation provided by data subjects at [LOCATION] and only use

the identification documentation provided by data subjects to respond to the data subject request and not for any other purpose. DPO must delete or destroy all identification after confirmation of the data subject's identity after six months.

8.4. DPO must confirm that the data subject provided the required information and verify the data subject's identity based on that information. If DPO cannot verify the data subject's identity based on the information provided, or if the data subject did not include all the required forms of identification DPO must advise the data subject in writing that we need additional information to verify the data subject's identity.

8.5. DPO should make clear when communicating with data subjects that the one-month time frame to respond to a data subject request does not start until we receive a fully completed request and proof of identity.

9. Requests Made on Data Subject's Behalf

9.1. A third party may make a request on a data subject's behalf. In this case, we require proof of the data subject's and third party's identity and evidence of the third party's legal right to act on the data subject's behalf.

9.2. We accept a photocopy or a scanned image of the following as proof of the data subject's identity: passport or photo identification such as a driver's licence, national identification number card, or birth or adoption certification. If data subjects changed their name, the third party must provide relevant documents evidencing the change.

9.3. We accept a photocopy or a scanned image of one of the following as proof of the third-party's identity: passport or photo identification such as a driver's licence, national identification number card and birth or adoption certificate.

9.4. We accept a copy of the following as proof of the third party's legal authority to act on the data subjects behalf: a written consent signed by the data subject, a certified copy of a Power of Attorney or evidence of parental responsibility.

9.5. We must store all documentation provided by third parties regarding their identity and legal authority to act on the data subject's behalf at [LOCATION] and only use that documentation to respond to the data subjects request and not for any other purpose. DPO must delete or destroy all identification and proof of legal authority documentation after confirmation of the third-party's identity and legal authority to act on the data subject's behalf.

9.6. DPO must verify the third party's identity and proof of legal authority to act on the data subject's behalf based on the information provided. If DPO cannot verify the third party's legal authority to act on the data subject's behalf, DPO must advise the third party in writing of the additional information needed to confirm the legal authority.

10. Identifying and Locating Relevant Personal Data

10.1 DPO is responsible for leading the effort to locate personal data relevant to a data subject request. DPO must:

(a) Identify all departments that might reasonably be considered to hold personal data relevant to the request.

(b) Work with the IT department to collect the personal data about the data subject from all relevant sources including:

i. emails, electronic files and documents and electronic systems
ii. databases
iii. automated systems such as door entry or key card access systems
iv. word processing systems
v. computer hard drives

vi. hard copy files
vii. voice recordings
viii. photographs
ix. monitoring records and CCTV images
x. internet logs
xi. telephone records
xii. back-up files
xiii. third-party data processors' systems

DPO must review the files and the documents collected and identify whether the information gathered is personal data relevant to the request.

If the scope of the data subject request is unclear or does not provide sufficient information to conduct a search (for example, the request asks for "all information about me"), DPO must communicate to the data subject that we need more specific information to process the request and locate the relevant personal data and indicate the information needed.

DPO must retain internal documents that show the steps and efforts made to locate relevant personal data, including all the search methods used.

11. Time to Respond to Data Subject Requests

11.1. DPO must respond to data subject requests no later than one month after receiving the request unless an exception applies.

11.2. If DPO determines that a data subject request may take longer than one month to respond to, DPO must notify the legal department via email. The legal department must determine if we can extend the one month response time.

11.3. If we extend the period for responding to the data subject request, DPO must inform the data subject within one month of receipt of the request of the extension and explain the reason(s) for the delay.

12. General Reasons for Denying a Data Subject Request

12.1. The Legal Department and DPO must determine if we have a basis not to respond to a data subject request. We may refuse to respond to a data subject request for the following reasons:

(a) A third party fails to present sufficient proof of authority to make the request on the data subject's behalf.

(b) When we process data for purposes that do not require data subject identification and we demonstrate that we cannot identify the data subject, we may deny data subject requests under Articles 15 (right of access), 16 (right to rectification), 17 (right to erasure), 18 (right to restrict processing) and 20 (right to data portability) unless the data subject provides additional information enabling identification.

(c) National Law provides a basis for denying the request.

(d) We demonstrate that the request is manifestly unfounded or excessive, in particular because of its repetitive character.

(e) We do not hold any personal data related to the data subject request.

12.2. These general grounds are in addition to the specific grounds for denying a request made under Articles 15 (right to access), 16 (right to rectification), 17 (right to erasure), 18 (right to restrict processing), 21 (right to object to processing) and 22 (automated processing exception) which are described in Paragraphs 14 through to 20.

12.3. Where we refuse to respond to a data subject's request DPO must explain the refusal to data subjects without undue delay and at the latest within one month after receipt of the request (unless a determination is made to extend the response deadline) and advise them of their right to complain to the supervisory authority and seek a judicial remedy.

12.4. If we do not have or process personal data related to the data subject, DPO should indicate that we conducted a diligent search for records related to the data subject's request and did not uncover responsive results.

13. Fees for Responding to Data Subject Requests

13.1. We must generally respond to a data subject's request for free. However, the GDPR permits us to charge a fee when requests are manifestly unfounded or excessive because of their repetitive character or when the request relates to large amounts of data.

13.2. DPO must determine whether we can charge a fee and the amount and then advise data subject's of that fee. DPO must document the reasons for charging the fee.

14. Responding to Personal Data Access Requests

14.1. Data subjects have the right to request access to their personal data processed by us under Article 15 of the GDPR.

14.2. In response to a data subject access request, DPO must, unless an exemption applies under Paragraphs 12 and 14.5, provide data subjects with the following information about our personal data processing activities or the specific data that they have requested:

(a) The purposes of processing.

(b) Categories of personal data processed.

(c) Recipients or categories of recipients who receive personal data from us.

(d) How long we store the personal data, or the criteria we use to determine retention periods.

(e) Information on the personal data's source if we do not collect it directly from the data subject.

(f) Information on the safeguards we use to secure transfers of personal data to non-EU countries or to an international organisation.

(g) Whether we use automated decision-making including profiling, the auto-decision logic used and the consequences of this processing.

(h) Their right to:

i. request correction or erasure of their personal data
ii. restrict or object to certain types of processing with respect to their personal data
iii. make a complaint with the local data protection authority

14.3. DPO must unless an exemption under Paragraphs 12 and 14.5 applies, provide the data subject with a copy of the personal data we process about the data subject in a commonly used electronic form.

14.4. Personal Data Pertaining to Third Parties:

(a) In certain cases, we process personal data that contains the personal data of several data subjects. The data subject access right must not adversely affect the rights and freedoms of

third parties.

(b) Where the data set includes third party's personal data, we must identify a legal basis under the GDPR prior to transferring the third party's data. The legal department and DPO must determine whether we have a basis to transfer the third party's data.

(c) In cases where the legal department and DPO determine that we do not have a basis to transfer the personal data of third party, the legal department and DPO may give instructions to redact or remove the personal data of the third party's prior to providing the data in response to an access request.

14.5. In addition to the general grounds for denying a data subject request set out in Paragraph 12, we may also refuse to respond to a data subject request if the data subject requests a copy of the personal data we process and providing a copy is likely to adversely affect the rights and freedoms of others.

14.6. The legal department and DPO must determine if we have a basis not to respond to a data subject access request. The legal department and DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

14.7. We may charge a reasonable fee if a data subject request additional copies of their data. DPO must determine whether we can charge a fee and the amount and advise the data subject of that fee in advance.

15. Responding to Correction (Rectification) Requests

15.1. Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data.

15.2. Where such a request is made, DPO must rectify the personal data without undue delay unless a basis exists under Paragraph 12 to deny the request.

15.3. DPO must identify each third-party recipient of the personal data that is the subject of the rectification. DPO must communicate the rectification of the personal data to each recipient (for example, our third-party service providers who process the data on our behalf), unless the Legal Department and DPO issues a written finding that it is impossible or involves disproportionate effort. DPO must also inform the data subject about those recipients if the data subject requests it.

15.4. The Legal Department and DPO must determine if we have a basis not to respond to the rectification request. DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

16. Responding to Erasure Requests

16.1. Data subjects have the right, in certain circumstances, to have their personal data erased. Where such a request is made, DPO must, unless an exemption applies under Paragraphs 12 and 16.4, erase the personal data that is the subject of the request.

(a) The personal data is no longer necessary for the purpose we collected it for.
(b) The data subject withdrew his or her consent to our processing activities and no other legal justification for processing applies.
(c) The data subject objects under GDPR Article 21(1) to:

i. Processing, including profiling, that is necessary for us to perform a task in the public interest or in the exercise of our official authority.
ii. There are no overriding legitimate grounds to process the personal data.

(d) The data subject objects under to processing under GDPR Article 21(2) for direct marketing

purposes.

(e) We unlawfully processed the data subject's personal data.

(f) EU or Member State Law requires us to erase the personal data to comply with a legal obligation.

(g) We collected the personal data in the context of offering online services to children by obtaining consent under GDPR Article 8(1).

16.2. If we determine that we must erase the data subject's data in response to the request and we made the personal data that is the subject of the erasure request public, DPO must take reasonable steps, including technical measures, to inform other organisations processing the personal data of the erasure request, including removing any links to, and copies of, the personal data.

16.3. If we determine that we must erase the data subject's data in response to the request, DPO must identify each recipient to whom we disclosed the personal data that is the subject of the erasure request.

DPO must communicate the erasure of personal data to the third-party data recipients, unless the legal department or DPO issues a written finding that this is impossible or involves disproportionate effort. DPO must also notify the data subjects about those recipients if they request that information.

16.4. In addition to the general grounds for denying a data subject request set out in Paragraph 12, we may also refuse to respond to a data subject erasure request if we process personal data that is necessary for:

(a) Exercising the right of freedom of expression and information.

(b) Complying with a legal obligation under EU or Member State Law.

(c) The performance of a task carried out in the public interest.

(d) Exercising our official authority.

(e) Public health reasons consistent with the exceptions for processing sensitive personal data such as health information, as outlined in GDPR Articles 9(2) (h) and (i) and 9(3).

(f) Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1), if the erasure is likely to render impossible or seriously impair the processing objectives.

(g) The establishment, exercise or defence of legal claims.

16.5. The legal department or DPO must determine if we have a basis not to respond to a data subject erasure request. The DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

17. Responding to Requests to Restrict Personal Data Processing

17.1. Data subjects have the right, in certain circumstances, to request that we restrict the processing of their personal data. Where such a request is made, DPO must unless an exemption under applies under Paragraph 12, restrict processing of the data subject's personal data if:

(a) The data subject contests the accuracy of the personal data. We must restrict processing the contested data until we can verify its accuracy.

(b) The processing is unlawful. Instead of requesting erasure of the data under Article 17, the data subject can request that we restrict use of the unlawfully processed personal data.

(c) We no longer need to process the personal data but the data subject needs the personal data for the establishment, exercise or defence of legal claims.

(d) A data subject objects to processing, including profiling, for:

i. Purposes that we consider necessary to perform a task in the public interest
ii. Purposes that we consider necessary for our or a third party's legitimate interests

17.2. If the data subject objects to processing under Paragraphs 17(d)(i) or 17(d)(ii), we must restrict the challenged processing activity pending verification of whether our or a third party's legitimate interests override the data subject's interests.

17.3. The Legal Department and DPO must determine if we have a basis not to respond to the data processing restriction request. DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

17.4. Where processing has been restricted, DPO must ensure that we only process the personal data (excluding storing it) either:

(a) With the data subject's consent.

(b) For the establishment, exercise or defence of legal claims.

(c) For the protection of the rights of another person.

(d) For reasons of important public interest.

17.5. DPO must inform the data subject that we intend to lift the restriction 30 days before lifting the restriction.

We may lift the processing restriction when:

(a) DPO verifies the accuracy of the personal data that is the subject of the processing restriction request.
(b) DPO Determines that our or a third party's legitimate interests override the data subject's interests if a data subject objects under Paragraphs 17(d)(i) or 17(d)(ii).

17.6. Where processing has been restricted, DPO must identify each recipient to whom we disclosed the personal data that is the subject of the processing restriction. DPO must communicate the processing restriction to the third-party data recipients, unless the legal department or DPO issues a written finding that it is impossible or involves disproportionate effort. DPO must also notify the data subjects about those recipients if they request that information.

18. Responding to Data Portability Requests

18.1. Data subjects have the right, in certain circumstances to:

(a) Receive a copy of certain personal data from us in a structured, commonly used and machine-readable format and store it for further personal use on a private device.

(b) Transmit certain personal data to another data controller.

(c) Request us to transmit certain personal data directly to another data controller, where technically possible.

18.2. The Data Portability Right only applies to personal data processed by automated means when processing is either:

(a) Based on the data subject's consent.

(b) Necessary to perform a contract with the data subject.

18.3. The personal data covered by the Data Portability Right includes only personal data concerning the data subject which the data subject knowingly and actively provided to The University of Law such as name, contact information, etc. The data portability right does not include data that we create from the data provided by the data subject such as a user profile. If you have any questions about whether personal data falls within the scope of a data subject portability request, please contact the DPO.

18.4. For personal that the data subject has requests to be transmitted to a third party, DPO must, unless an exemption applies under Paragraphs 12 and 18.7, transfer the personal data that is the subject of the Data Portability Request. However, if the data subject requests a particular format, DPO should make efforts to transfer the data in that format.

18.5. For portability requests asking that the personal data to be transmitted directly to the data subject, DPO must, unless an exemption applies under Paragraphs 12 and 18.7, transfer the personal data that is the subject of the Data Portability. However, if the data subject requests a particular format, DPO should make efforts to transfer the data in that format.

18.6. Personal Data Pertaining to Third Party's:

(a) Where the data set includes third party's personal data we must identify a legal basis under the GDPR prior to transferring the third party's data. The legal department and DPO must determine whether we have a basis to transfer the third party's data.

(b) In cases where the legal department and DPO determine that we do not have a basis to transfer the personal data of third party's, the legal department or DPO may give instructions to redact or remove the personal data of the third party prior to transmitting the data in response to a portability request.

18.7. In addition to the general grounds for denying a data subject request set out in Paragraph 12, we may also refuse to respond to a data subject portability request if responding to the request adversely affects the rights and freedoms of others.

18.8. The Legal Department and DPO must determine if we have a basis not to respond to a Data Portability request. DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

18.9. Data subjects have the right to object to personal data processing when we process their personal data:

(a) For direct marketing purposes, including profiling related to direct marketing. We must stop processing a data subject's personal data for direct marketing purposes whenever the data subject objects.

(b) For scientific or historical research purposes or statistical purposes, subject to the exceptions described in Paragraph 19.5(a).

(c) Based on GDPR Articles 6(1)(e) (processing for a task carried out in the public interest or the exercise of official authority vested in us) or 6(1)(f) (processing necessary for the legitimate interests of us or a third party).

18.10. DPO must, unless an exemption applies under Paragraphs 12 and 19.3 stop the personal data processing related to the data subject's request.

18.11. In addition to the general grounds for denying a data subject request set out in Paragraph 12, we can refuse to grant a data subject processing objection when:

(a) A data subject objects to processing for scientific or historical research purposes or statistical purposes and we demonstrate that the processing is necessary for us to perform a task in the public interest.

(b) A data subject objects to processing, including profiling, based on Articles 6(1)(e) (processing for a task carried out in the public interest or the exercise of official authority vested in us) or 6(1)(f) (processing necessary for the legitimate interests of us or a third party) and we demonstrate:

i. A compelling legitimate ground for processing the personal data that overrides the data subject's interests

ii. That we need to process the personal data to establish, exercise or defend legal claims.

18.12. For objections to data processing based on Paragraph 19.3(b), we must temporarily restrict processing that personal data in accordance with Paragraph 17 pending verification of whether our legitimate interests override those of the data subject.

18.13. If the Legal Department and DPO determine that there are no overriding legitimate grounds for the personal data processing under Paragraph 19.3(b), DPO must erase that personal data in accordance with Paragraph 16.

18.14. The legal department and DPO must determine if we have a basis not to respond to a data subject objection request. DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

19. Responding to Automated Decision-Making Objections

19.1. Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, including profiling, if the decision produces legal or other similarly significant effects on them.

19.2. The Legal Department and DPO must determine if the automated decision-making, including profiling, produces legal effects on the data subject or affects them in a similarly significant way.

19.3. DPO must, unless an exemption applies under Paragraphs 12 and 20.4, stop the automated decision-making that is the subject of the data subject request.

19.4. In addition to the general grounds for denying a data subject request set out in Paragraph 12, we can refuse to grant an automated decision-making objection when the automated decision is either:

(a) Necessary for entering into or performing a contract with the data subject.

(b) Authorised by EU or Member State Law applicable to us.

(c) Based on the data subject's explicit consent.

19.5. The Legal Department and DPO must determine if we have a basis not to respond to the data subject's automated decision-making objection. DPO must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

The University of Law does not currently process any data on a solely automated basis.

20. Training and Awareness

20.1. This policy will be published on The University of Law website. DPO must ensure that all staff subject to the Policy understand their roles in implementing this policy through training, communications and team meetings.

21. Enforcement

21.1 Violations of or actions contrary to this policy may result in disciplinary action, in accordance with The University of Law Information Security Policies and Procedures and Human Resources Policies.

Version	Date	Author	RevisionSummary
V.01	09/2019	DPO	