Ferris State University
General Data Protection Regulation (GDPR) Policy

1 PURPOSE

The European Union ("**EU**") General Data Protection Regulation ("**GDPR**") requires Ferris State University ("**Ferris**") to have in place appropriate safeguards to protect information relating to an identified or identifiable natural person residing in the European Economic Area ("**Personal Data**"). Ferris' policy is to establish and maintain appropriate safeguards and controls related to the Processing of Personal Data as required by the GDPR ("**Processing/Processed**"). Processing and or Processed under GDPR means any operation performed on Personal Data, including but not limited to collection, use, disclosure, storage, retrieval, erasure or destruction. This Policy sets forth the expected behaviors of Ferris and its workforce members relating to the Processing of any Personal Data belonging to Ferris or a third party (i.e., a Data Subject).

2 SCOPE AND POLICY STATEMENT

This Policy applies to all Personal Data Processed in electronic or physical form by or on behalf of Ferris, and applies to all Ferris workforce members responsible for such Processing. Capitalized terms not defined in this Policy have been defined by GDPR. This Policy does not override any other applicable data privacy laws that apply to Ferris.

Ferris is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct. Ferris, as a Controller under the GDPR, is responsible for ensuring compliance with GDPR and the data protection requirements outlined in this Policy. Noncompliance may expose Ferris to complaints, regulatory action, fines and/or reputational damage. Ferris' leadership is fully committed to ensuring continued and effective implementation of this Policy and expects all Ferris workforce members to share in this commitment.

Ferris has in place a consistent level of data protection and security measures across its organization, including the protections and procedures contained in its Information Security Policy and Guidelines and HIPAA Policies & Procedures. Ferris has also established additional procedures for the Processing of Personal Data. The purpose of this Policy is to address the protections and rights that individuals have in regards to the Processing of their Personal Data and how Ferris is continuously working to maintain these protections and rights.

3 DEFINITIONS

For the purposes of this Policy:

(a) *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.

(b) *Controller* means the natural or legal person, public authority, agency, or other body, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(c) *Data Subject* means an identified or identifiable natural person, which 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.

(d) *Personal Data Breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

(e) *Processor* means a natural or legal person, public authority, agency, or other body, which Processes Personal Data on behalf of the Controller.

(f) *Special Categories of Personal Data* means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data or data concerning a natural person's sex life or sexual orientation, Genetic Data, or Biometric Data. *Genetic Data* means 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. *Biometric Data* mean Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

(g) *Supervisory Authority* means a supervisory authority which is concerned by the Processing of personal data because: (a) the Controller or Processor is established in the territory of the Member State of that supervisory authority; (b) Data Subjects residing in the Member State of that supervisory authority are substantially affected or likely to be affected by the Processing; or (c) a complaint has been lodged with that supervisory authority.

4 GDPR DATA PROTECTION PRINCIPLES AND COMPLIANCE MEASURES

Article 5 of GDPR sets forth six data protection principles for Personal Data that Ferris must abide by to comply with the GDPR:

(1) Personal Data must be Processed lawfully, fairly, and in a transparent manner;

(2) Personal Data should only be collected for specified, explicit, and legitimate purposes;
(3) Personal Data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed;
(4) Personal Data must be accurate and, where necessary, kept up to date;
(5) Personal Data must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed; and
(6) Personal Data must be Processed in a manner that ensures the appropriate security of Personal Data at all stages of the Personal Data lifecycle, including using appropriate technical and organizational measures to protect against unauthorized or unlawful Processing and against accidental loss, destruction, or damage.

Thus, GDPR requires Controllers like Ferris to provide detailed, specific information to Data Subjects about their Personal Data. This information includes the identity of the Controller and how and why Ferris will Process, protect, and retain the Personal Data. This information must be presented to the Data Subject when the Data Subject first provides his or her Personal Data to Ferris.

The following sections are designed to address Ferris' GDPR compliance efforts in greater detail.

A. <u>Policies and Procedures</u>
Ferris must implement the appropriate technical and organizational measures to ensure that Data Subjects' rights are protected. Ferris has developed its Information Security Policy and Guidelines Policies and Procedures, and its Website Policy and Procedures to fulfill the requirements and standards under the GDPR and other relevant data protection laws. These Policies and Procedures specifically address the mechanics of how Ferris protects and retains various categories of information, including Personal Data.

B. <u>Legal Basis for Processing</u>
Ferris must review all Processing activities to identify the legal basis for Processing and ensure that each basis is appropriate for the activity to which it corresponds. Legal purposes for Processing Personal Data include: consent; Processing necessary for the performance of a contract between Ferris and the Data Subject or Controller; Processing necessary to meet Ferris' legal compliance obligations; Processing necessary to protect a Data Subject's vital interests; or Processing necessary for Ferris to pursue its legitimate interests, as long as such interests are not overridden by the interests or fundamental rights and freedoms of the Data Subject. Additionally, Ferris must continually audit its Processing activities to ensure that the legal bases for such Processing are accurate and up to date.

C. <u>Obtaining Consent from Data Subjects</u>
In those circumstances when Ferris relies on consent to Process any Personal Data, Ferris's consent mechanisms for obtaining Personal Data from Data Subjects must

ensure that the individuals understand when they are providing Consent and why and how Ferris uses the information Processed with their Consent. Consent requires an affirmative action on the part of the Data Subject, and must be clearly indicated, either by a statement or a positive action to the Processing. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honored. Ferris will keep records of all consents of Data Subjects in accordance with Subsection H, below.

D. Direct Marketing

Ferris may send direct marketing communications to a Data Subject only with the Data Subject's prior opt-in Consent where another legal basis for sending the communication is not clearly established. In all cases, including where prior opt-in Consent of the Data Subject is not required, Ferris shall offer the Data Subject the opportunity to opt-out of such direct marketing communications. If a Data Subject objects to receiving marketing communications from Ferris, or withdraws his or her Consent to receive such communications, Ferris will take steps to refrain from sending further marketing within the time period required by the GDPR and other applicable law.

E. Data Protection Impact Assessments

When Ferris seeks to implement new technologies in how it Processes Personal Data, it will evaluate whether it needs to conduct an assessment of the impact of the new Processing operations (a "**Data Protection Impact Assessment**" or "**DPIA**") to determine the level of risk associated with the new Processing activity and whether a new legal basis for such Processing is required. A DPIA is required when the new Processing activity is likely to result in a high risk to the rights and freedoms of natural persons. Examples of when a DPIA is required include the following cases:

- a systematic and extensive evaluation of personal aspects relating to Data Subjects based on automated Processing, including profiling, and on which decisions are based that produce legal effects concerning or otherwise significantly affecting the Data Subject;
- Processing special categories of Personal Data (see Subsections I and J) on a large scale; or
- a systematic monitoring of a publicly accessible area on a large scale.

DPIAs will allow Ferris to rate the risk posed by the Processing activity and implement mitigating measures to reduce the risk posed to Data Subjects. DPIAs will be conducted with the involvement of the Data Privacy and Security Committee (the "**Committee**") and a record of the results will be maintained in line with Subsection H.

F. Third-Party Processors

When Ferris engages third parties to Process Personal Data on its behalf (each, a "**Third Party Processor**"), Ferris shall follow its due diligence procedures to confirm that such Third Party Processors are Processing Personal Data properly and according to GDPR. This includes putting in place a Data Processing Agreement (as more fully described in Subsection G, below) and monitoring its Third Party Processors' security standards and GDPR compliance efforts.

G. Data Processing Agreements

For the purposes of this Policy, "**Data Processing Agreement**" or "**DPA**" means a GDPR-compliant agreement for Processing Personal Data. When Ferris desires to engage Third Party Processors, Ferris shall put in place DPAs to ensure the Third Party Processors meet and understand Ferris' GDPR obligations as well as their own. Ferris will not transfer Personal Data to Third Party Processors that cannot comply with a DPA and that do not agree to put adequate compliance measures in place.

H. Record Keeping

Ferris must keep full and accurate records of all of its data Processing activities, including records of Data Subjects' consents and Ferris's procedures for obtaining consents when Ferris is acting as a Controller. The records shall include, at a minimum, clear descriptions of: the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage location, Personal Data transfers, the Personal Data's retention period, and a description of the security measures in place. All of the records described above will be kept in compliance with the following:

i. *Documenting Policies and Procedures*. Ferris will maintain a copy of this Policy for six years beyond the date the documents cease to be effective.

ii. *Documenting Authorizations and Responses to Exercise Individual Rights*. Ferris will maintain for a period of six years from the date the document was last effective, the following documents:

- individual consents for the Processing of Personal Data;
- requests to exercise individual rights related to Ferris' Processing activities (see Section 5, below), and the related response to the request, which will be maintained for six years beyond the date of the most recent entry on the form, and which shall include:
  - the individual whose Personal Data was disclosed;
  - the date of the disclosure; and
  - a brief statement of the request, purpose for the disclosure, and Personal Data disclosed; and
- if Ferris elects not to grant an individual's request, Ferris must maintain legal justification of such denial for a period of six years from the date of denial.

In addition to the documents listed above, Ferris may at its discretion maintain any additional documents it believes are appropriate relating to requests by individuals to exercise their individual rights under GDPR.

The obligation to retain documents relating to individual rights is limited to requests made to Ferris for documents maintained by Ferris. When Personal

Data is held by a Ferris third party service provider, Ferris will work with the service provide to ensure Ferris properly maintains the required documentation relating to individual rights.

iii. *Documenting Personal Data Breaches.* Ferris will maintain for a period of six years from the date a Personal Data Breach was fully resolved, the following documents:

- a summary of the Data Breach that would enable the Supervisory Authority to verify compliance with GDPR, including:
  - the relevant facts related to the Personal Data Breach;
  - the effects (or anticipated effects) of the Personal Data Breach;
  - the remedial actions taken by Ferris;
  - whether Ferris notified anyone of the breach (and the categories of persons notified);
  - if notification to any party was delayed, the reasons for such delay; and
- if Ferris determines notification is necessary, a copy of the notices sent to the Supervisory Authority and Data Subjects; or
- if Ferris determines it does not need to notify the Supervisory Authority or any Data Subjects, the rationale behind Ferris' determination.

iv. *Documenting Data Processing Agreements*. Ferris will maintain copies of all DPAs with all Third-Party Processors for a period of six years from the date the contract was last in effect.

v. *Documenting Training*. Ferris will maintain documentation demonstrating the dates when employees with access to Data were trained concerning the Privacy Rules and any applicable Policies and Procedures, for a period of six years from the date each training session was concluded.

vi. *Documenting Complaints*. Ferris will maintain documentation of all complaints that Ferris receives of violations of this Policy or GDPR, and all documentation relating to disposition of the complaints. Ferris will maintain these documents for six years from the date of a complaint's final disposition.

vii. *Documenting Disciplinary Action*. Ferris will maintain documentation of all disciplinary action that Ferris has taken against employees for violations of this Policy or GDPR, for a period of six years from the date of the disciplinary action.

viii. *Documenting Mitigation Efforts*. Ferris will maintain all documents relating to Ferris' efforts to minimize the harmful effects of any unauthorized Processing for a period of six years from the date of the action. Such documentation will include known details of the unauthorized Processing, details of Ferris' efforts to retrieve Personal Data or halt the improper Processing, and all correspondence relating to the unauthorized Processing.

I. Special Categories of Personal Data

When Ferris Processes Special Categories of Personal Data under GDPR, including race and ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, biometric data used to identify an individual, genetic data, health data, or data related to sexual preferences and/or sexual orientation, it must do so only when necessary and when Ferris has first identified the appropriate legal basis for Processing such Personal Data.

Permissible legal bases for Processing Special Categories of Personal Data are set forth under Article 9 of the GDPR and include Processing necessary to establish, exercise or defend legal claims or Processing with the express consent of the Data Subject. Where Ferris relies on consent for Processing, it must ensure the consent is explicit and is verified by a signature, with the right to modify or remove consent being clearly communicated in writing.

Ferris will protect and store all Special Categories of Personal Data in accordance with its Information Security Policy and Guidelines.

J. Personal Data Related to Criminal Convictions

Personal Data related to criminal convictions is subject to strict requirements under Article 10 of the GDPR; therefore, Processing of this type of Personal Data requires approval by Ferris' General Counsel. Ferris may only Process Personal Data related to criminal convictions and offenses if it has consent from the Data Subject to do so and if such Processing is carried out only under the control of an official authority or the Processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects. Information related to criminal convictions and offenses must be protected and stored by Ferris in accordance with its Information Security Policy and Guidelines.

K. Transferring Personal Data Across Borders

Ferris may not transfer Personal Data outside of the European Union unless there are appropriate safeguards between the parties or the European Commission has determined that the country outside the European Union ensures an adequate level of protection. For transfers from the European Union to the United States, appropriate safeguards include Privacy Shield certification by the United States recipient or Standard Contractual Clauses in addition to a Data Processing Agreement (see Subsection G).

5 RESPONDING TO DATA SUBJECTS

Ferris recognizes that Data Subjects have certain rights under GDPR related to the Processing of their Personal Data. These include rights to:

- request access to their Personal Data that Ferris holds (Article 15);

- correct, or ask Ferris to correct, the Personal Data that Ferris holds (Article 16);
- ask Ferris to erase Personal Data (Article 17);
- in certain circumstances, restrict Ferris' Processing (Article 18) or object to Ferris' Processing activities entirely (Articles 21-22); and
- receive a copy of their Personal Data or ask for their Personal Data to be transferred to a third party (Article 20).

The following general points apply to all of the requests of Data Subjects:

- Ferris will strive to provide information to the individual in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.
- Information should be provided to a Data Subject in writing, or electronically by other means, even if the original request is submitted orally, such as over the phone or face to face.
- Ferris shall act on a request from an individual unless Ferris is unable to establish his or her identity.
- Ferris shall provide information without delay (within one month from the date of request).
- The response timetable may be extended by an additional two months for complex or a high volume of requests. The individual must be informed of this extension and the reasons for this extension before the end of the initial one-month period.
- If it is decided that Ferris will not comply with a request, Ferris must inform the individual without delay, stating the reason(s) and informing the individual of their right to complain to a supervisory authority.
- Generally, responses to requests will be made free of charge, unless they are unfounded or excessive, in which case Ferris will either charge a reasonable fee or refuse to fulfill the request.
- If there is doubt about an individual's identity, Ferris may request further information to establish it.

A. Tracking Data Subject Requests

All Data Subject requests received by Ferris should be forwarded immediately to the privacy@ferris.edu email address. The Committee must track the following information regarding Data Subject requests in accordance with Section 4.H.i:

- Receipt date of Data Subject request.
- Data subject name.
- Requester name (if applicable).
- Email address, phone number, or other contact information to respond to a Data Subject's request.
- Individual assigned to handling Data Subject request.
- Request status (new, in progress, completed).
- Request format.
- Request type.
- Request details.
- Final response date.
- Final disposition.

B. Verifying the Identity of Individuals

Ferris' first step to responding to Data Subjects' rights requests is verifying the identity of the Data Subject submitting the request as follows:

i. *In Person*. If the Data Subject making the request is not known to the Ferris employee receiving the request, the employee will take appropriate steps to verify the identity of the Data Subject which may include reviewing and making a copy of a valid photo identification issued by a government agency.

ii. *By Telephone*. If the Data Subject requests Personal Data over the telephone and the employee is reasonably able to positively identify the Data Subject over the telephone, no further verification is required. Ferris may request that the Data Subject provide his or her address, telephone number, and other Personal Data that Ferris has on file to confirm his/her identity. If the employee cannot verify the identity of the Data Subject, the employee will instruct the Data Subject to make the request in person, or direct the Data Subject to send the request in writing.

iii. *By Email*. If the Data Subject makes the request through email:

- From within Ferris' email system: If the request is from a Ferris employee or student and originates within the Ferris email system, the email is considered authenticated because of the log-in procedures that the employee must use to gain access to his or her account through the Ferris email system. Ferris employees receiving such requests will be trained on the risk of compromised emails.
- From outside the Ferris email system: If the request from a Data Subject originates from another email system or a public email service (e.g. yahoo.com), the person receiving the request must verify the authenticity of the email. If it is not possible to verify the authenticity of the email, the Data Subject should be asked for additional, non-sensitive Personal Data such as address, telephone number, and other Personal Data that Ferris has on file. The additional information should then be compared with the Personal Data Ferris has on record. If the Personal Data does not match, or if there is any doubt as to the identity of the person making the request, contact the Committee, as appropriate.

iv. *In Writing*. If the individual submits a written request for Personal Data, compare the Personal Data provided in the written request with Personal Data Ferris has on record. If the Personal Data does not match, or if there is any doubt as to the identity of the person making the request, contact the Committee through the privacy@ferris.edu email address, as appropriate. Ferris may develop a form to use for written requests.

C. Identifying and Locating Relevant Data

The Committee will identify the departments that might reasonably be considered to hold Personal Data relevant to the request. Ferris General Counsel will be informed of any Data Subject request that involves searching through Ferris student data. The relevant department leader will work to collect the Personal Data about the Data Subject from all relevant sources, including, but not limited to, emails, electronic files and documents, and electronic systems, databases, and hard copy files. This may also include submitting a formal request to obtain a student file. The Committee will retain internal documents that show the steps and efforts made to locate relevant Personal Data.

D. <u>Responding to Data Subject Rights Requests</u>

In responding to all the Data Subject rights requests laid out below, the Committee will determine whether Ferris has a legal basis under the GDPR not to respond to a Data Subject's request (see Section 5.E, below). If Ferris denies a Data Subject's request, it must inform the Data Subject of the reason for the denial and of the individual's ability to file a complaint with a supervisory authority (the data protection authority for the relevant member state) and seek a judicial remedy. Note that the procedures set forth below assume Ferris is acting as a Controller. If Ferris believes it is acting as a Processor it should consult with legal counsel prior to responding to a Data Subject's request, as Ferris' position as a Processor will require Ferris to work with the Controller in responding to the Data Subject's request.

i. Responding to Personal Data Access Requests

Data Subjects have the right to request access to their Personal Data Processed by Ferris under the GDPR. In response to a Data Subject access request, the Committee must, unless an exemption applies under Section 5.E, provide Data Subjects with the following information about Ferris's Personal Data Processing activities:

- The purposes of Processing.
- Categories of Personal Data Processed.
- Recipients or categories of recipients who receive Personal Data from Ferris.
- How long Ferris stores the Personal Data, or the criteria Ferris uses to determine retention periods.
- Information on the data source if Ferris does not collect it directly from the Data Subject.
- Information on the safeguards Ferris uses to secure transfers of Personal Data to non-EU countries or to an international organization.
- Whether Ferris uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this Processing.
- The Data Subject's right to:
  - request correction or erasure of their Personal Data;
  - restrict or object to certain types of Processing with respect to their Personal Data; and
  - make a complaint with the local data protection authority.

Unless an exemption applies under Section 5.E, the Committee must provide the Data Subject with a copy of the Personal Data Ferris Processes about the Data Subject in a commonly used electronic form.

ii. *Responding to Personal Data Correction (Rectification) Requests*

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. Where such a request is made, the Committee must rectify the Personal Data without undue delay unless a basis exists under Section 5.E to deny the request.

iii. *Responding to Erasure Requests*

Data Subjects have the right, in certain circumstances described below, to have Ferris erase their Personal Data. Where such a request is made, the Committee must, unless a basis exists under Section 5.E to deny the request, erase the Personal Data that is the subject of the request if:

- the Personal Data is no longer necessary for the purpose Ferris collected it;
- the Data Subject withdrew consent to Ferris' Processing activities and no other legal justification for Processing applies;
- Ferris unlawfully Processed the Personal Data; or
- EU or member state law requires Ferris to erase the Personal Data to comply with a legal obligation.

If Ferris determines that it must erase the Personal Data in response to the request, the Committee must identify each recipient to whom Ferris disclosed the Personal Data that is the subject of the erasure request. The Committee must instruct the Processor to erase the Personal Data. The Committee must also notify the Data Subjects about Ferris' Processors if they request information regarding other parties with access to their Personal Data.

In regard to the right to erasure specifically, Ferris may refuse to implement a Data Subject erasure request if Ferris Processes Personal Data that is necessary for one of the following reasons, provided that Ferris must still inform the Data subject that it is unable to fulfill the request based on such reason:

- Exercising the right of freedom of expression or information.
- Complying with a legal obligation under EU or member state law or performing of a task carried out in the public interest.
- For reasons of public interest related to public health.
- For scientific or historical research or statistical purposes that are in the public interest, where such purpose would be seriously impaired if the erasure request was fulfilled.
- Establishing, exercising, or defending legal claims.

iv. *Responding to Objections to, or Requests to Restrict, Personal Data Processing*

Data Subjects have the right to request that Ferris restricts the Processing of their Personal Data or object to the Processing of Personal Data outright. Unless a basis exists under the "Denying a Data Subject Request" section of this Policy to deny such request, Ferris must restrict Processing of the Personal Data if:

- The Data Subject contests the accuracy of the Personal Data. Ferris must restrict Processing the contested data until Ferris can verify its accuracy.
- The Processing is unlawful.
- Ferris no longer needs to Process the Personal Data, but the Data Subject needs the Personal Data for the establishment, exercise, or defense of legal claims.
- A Data Subject objects to Processing, even if the Processing is necessary for Ferris to perform a task in the public interest or to pursue Ferris' or a third party's legitimate interests, if there are no overriding legitimate grounds to Process the Personal Data.
- the Data Subject objects under GDPR Article 21(2) to Processing for direct marketing purposes.

Where the Committee determines the restriction of Processing is appropriate, the Committee must ensure that Ferris only Processes Personal Data either:

- With the Data Subject's consent.
- For the establishment, exercise, or defense of legal claims.
- For the protection of the rights of another person.
- For reasons of important public interest.

v. *Responding to Data Portability Requests*

In the circumstances described below, Data Subjects have the right to:

- Receive a copy of certain Personal Data from Ferris in a commonly used and machine-readable format and store it for further personal use on a private device.
- Transmit certain Personal Data to another Controller.
- Have Ferris transmit certain Personal Data directly to another Controller, where technically possible.

The right to data portability only applies to Personal Data that is Processed by automated means, when Processing is either (1) based on the Data Subject's consent; or (2) necessary to perform a contract with the Data Subject. Furthermore, the Personal Data covered by the right to data portability includes only Personal Data that the Data Subject knowingly and voluntarily provided to Ferris, such as name and contact information. It does not include data that Ferris creates from the information provided by the Data Subject.

Unless an exemption applies under Section 5.E, the Committee must transfer the Personal Data that the Data Subject is requesting in a commonly used electronic format, or other format the Data Subject requests, so long as that format is reasonable.

E. Denying a Data Subject Request

i. *Generally.*

Ferris will determine if it has a basis to deny a Data Subject request. Ferris may refuse to implement a Data Subject request for the following reasons:

- The Data Subject fails to provide sufficient proof for Ferris to verify his or her identity, or a third party fails to present sufficient proof of authority to make the request on the Data Subject's behalf.
- Privacy laws provide a basis for denying the request.
- Ferris does not have any Personal Data related to the Data Subject's request.
- The Data Subject's request is unfounded or excessive, in particular because of its repetitiveness.

When Ferris does not fulfill a Data Subject's request, it must explain the refusal to the Data Subject 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. A response deadline may be extended if Ferris does not have adequate information from the Data Subject to fulfill the request or if the Data Subject's request is complex and implicates Personal Data in Ferris' capacity as a Controller and Processor. In Ferris' response, it must also advise Data Subjects of their right to complain to a supervisory authority and seek a judicial remedy.

If Ferris denies a request, it should document the denial, including the legal justification for such denial, in accordance with Section 4.H.

ii. *No Personal Data Related to a Data Subject Request*

If Ferris does not have or Process Personal Data related to a Data Subject, Ferris should notify the Data Subject that it conducted a diligent search for records related to the Data Subject's request and did not uncover responsive results.

Ferris should keep all records related to the Data Subject's request and any internal documents detailing the steps that Ferris took to locate the Personal Data, including the search methods utilized, in accordance with Section 4.H.

F. Fees for Responding to Data Subject Requests

Ferris must generally respond to a Data Subject request for free. However, Ferris may charge a fee when requests are manifestly unfounded or excessive, either because of their repetitive character or when the requests relate to large amounts of data.

6 REPORTING A PERSONAL DATA BREACH

In the event that Ferris becomes aware of a Personal Data Breach, Ferris will follow the same procedures set forth in its HIPAA Breach Notification Policy, subject to the following additional requirements:

A. Notification to Supervisory Authorities
Ferris will notify the applicable Supervisory Authority within 72 hours after becoming aware of the Personal Data Breach, unless Ferris determines that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, using a similar analysis as set forth in the HIPAA Breach Notification Policy related to determining whether data has been compromised. If any delay in reporting is necessary, the reasons for this delay must be communicated to the Supervisory Authority. In all cases, external reporting must be conducted within thirty (30) days.

Notification to authorities must: (i) describe the nature of the Personal Data Breach including where possible, the categories and the approximate number of Data Subjects concerned, and the categories and the approximate number of Personal Data records concerned; (ii) include the name and contact details of a Ferris point of contact where more information can be obtained; (iii) describe the likely consequences of the Personal Data Breach; and (iv) describe the measures taken or proposed to be taken by Ferris to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. If it is not possible to provide all necessary information at the same time, the information may be provided in phases, without undue delay.

B. Notification to Data Subjects
If Ferris determined that the Personal Data Breach is likely to result in a high risk to Data Subjects, notification to such Data Subjects is also required, and such notice should align with the HIPAA Breach Notification Policy related to notification to individuals, but must also include the name of the Committee and contact information for the privacy@ferris.edu email.

Affected Data Subjects must be notified in the most expedient time possible, and without unreasonable delay, consistent with any measures necessary to determine the scope of the Personal Data Breach and to restore the reasonable integrity of the data system. Delay is permitted when a law enforcement agency has determined that notification will impede a criminal investigation. In such case, notification must occur as soon as the law enforcement agency determines that notification will no longer compromise the investigation. The factors considered when determining the timing of notification must be documented in accordance with Section 4.H.

C. Documentation

Ferris must document the details of any Personal Data Breach, including the notifications sent out or Ferris' reasoning for not sending notification, in accordance with Section 4.H.

7 CHANGES TO THIS POLICY

Ferris will regularly review this Policy and update it as appropriate.

If you have any questions about this Policy, please contact Ferris' Data Privacy and Security Committee at (231) 591-2331 or privacy@ferris.edu.