POLICY ON HANDLING DATA SUBJECT REQUESTS

1. DEFINITIONS AND INTERPRETATION

This Policy uses certain key terms, which mean the following:

Data controller means the natural or legal person that determines the purposes and means of processing personal data, or Millennium Point. This Policy only applies when Millennium Point acts as a data controller and not when the organisation acts as a data processor, as defined below.

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

Data processor means a natural or legal person that processes personal data (defined below) on behalf of a data controller such as Millennium Point's third-party vendors or affiliates, subsidiaries, and related corporate entities providing services. Millennium Point may act as a data processor in certain situations for affiliates, related corporate entities, and third parties. However, this Policy does not apply to Millennium Point's personal data processing activities as a data processor. If you have any questions about whether Millennium Point is acting as a data controller or a data processor, please contact the GDPR Compliance Manager.

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

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 or information, which relates to an individual.

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.

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.

The rights of data subjects covered in this policy only directly apply to us to the extent that we act as a data controller in relation to the data subjects personal data.

Where and to the extent that we act as a data processor of a data subject's personal data, then these rights do not directly apply to us, but we may still have to comply with them as the request may also be made or be treated as being made to the data controller, and we then have to indirectly comply on their behalf.

2. PURPOSE

2.1 Millennium Point 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:

2.1.1 Access their personal data under GDPR Article 15.

2.1.2 Correct their personal data under GDPR Article 16.

2.1.3 Erase their personal data under GDPR Article 17.

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

2.1.5 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.

2.1.6 Object to personal data processing under GDPR Article 21.

2.1.7 Not be subject to automated decision-making in certain circumstances under GDPR Article 22.

2.2 The purpose of the Policy is to formalize procedures for:

2.2.1 Confirming the identity of the data subject making a request or the identity of the third party making a request on a data subject's behalf.

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

2.2.3 Identifying and locating relevant personal data.

2.2.4 Determining whether a GDPR or other exemption exists that permits or requires us to refuse to fulfil the request or limits the extent to which we need to comply.

2.2.5 Handling data subject requests that involve several data subjects' personal data.

2.2.6 Communicating with data subjects at reasonable intervals regarding the status of their request.

3. SCOPE

3.1 This Policy applies to all of Millennium Point's employees. The department responsible for handling these requests is the People, Learning and Development department and GDPR Compliance Manager.

4. DATA SUBJECT REQUEST SUBMISSION FORMAT

4.1 All data subjects seeking to exercise their rights under the GDPR may submit their request in any form, both in writing and orally.

4.2 If you receive an oral data subject request, direct the data subject to submit the request via the GDPR Compliance Manager (gdprcompliancemanager@millenniumpoint.org.uk)

5. TRACKING DATA SUBJECT REQUESTS

5.1 All data subject requests received must be forwarded to the GDPR Compliance Manager and People Learning and Development department.

5.2 The GDPR Compliance Manager / PLD Department must maintain all correspondence and documentation related to data subject requests at Millennium Point Property Limited.

6. ACKNOWLEDGING RECEIPT OF DATA SUBJECT REQUESTS

6.1 The GDPR Compliance Manager / PLD department must advise the data subject in writing electronically via email that Millennium Point received the request and that the data subject should expect to receive a response within one month.

7. INVOLVE RELEVANT DEPARTMENTS

7.1 The GDPR Compliance Manager must provide the data subject request to the PLD department via e-mail 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 It is essential that this is done quickly, as the normal legal deadline to comply with the request is at most one month, so there may be a lot of work to be done in order to comply so the request needs to be brought to the attention of relevant individuals as soon as possible.

7.3 The PLD department must assign an individual or individuals to handle the data subject request.

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 we are not sure of their identity.

8.2 Data subjects, whose identity we are not sure of, 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 license, national identification number card, or birth or adoption certification. If a data subject has changed their name, they must provide relevant documents evidencing the change.

8.3 We must store all identification documentation provided by data subjects at Millennium Point Property Limited and only use the identification documentation provided by data subjects to respond to the data subject request and not for any other purpose. The People, Learning and Development department must delete or destroy all identification after 6 years from the date we complied with the request.

8.4 The People, Learning and Development department must confirm that the data subject provided the required information and verify the data subject's identity based on that information. If the People, Learning and Development department 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, the People, Learning and Development department must advise the data subject in writing that we need additional information to verify the data subject's identity.

8.5 The People, Learning and Development department should make clear when communicating with data subjects that the one-month period to respond to a data subject request does not start until we receive a fully completed proof of identity where this is required.

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 may 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 license, national identification number card, or birth or adoption certification. If a data subject has 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 license, national identification number card, or 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 subject's behalf: a written consent signed by the data subject, a certified copy of a Power of Attorney, or evidence of parental responsibility. We must be able to link the authorisation to the data subject, e.g. by matching the signature on a copy passport to the signature on the authorisation.

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 Millennium Point Property Limited and only use that documentation to respond to the data subject request and not for any other purpose. The People, Learning and Development department must delete or destroy all identification and proof of legal authority documentation after 6 years from the date we complied with the request.

9.6 The People, Learning and Development department 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 the People, Learning and Development department cannot verify the third party's legal authority to act on the data subject's behalf, the People, Learning and Development department 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 The GDPR Compliance manager and People, Learning and Development department is responsible for leading the effort to locate personal data relevant to a data subject request. They must:

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

10.1.2 Work with our out-sourced IT provider where possible to collect the personal data about the data subject from all relevant sources including:

(a) emails, electronic files and documents, and electronic systems;

(b) databases;

(c) automated systems such as door entry or key card access systems;

(d) word processing systems;

(e) computer hard drives;

(f) hard copy files;

(g) voice recordings;

(h) photographs;

(i) monitoring records and CCTV images;

(j) internet logs;

(k) telephone records;

(l) back-up files; and

(m) third-party data processors' systems.

10.2 The GDPR Compliance Manager and People, Learning and Development department must review the files and the documents collected and identify whether the information gathered is personal data relevant to the request.

10.3 A reasonable search of the relevant systems using the individual's name, employee or customer number, address, national insurance number, telephone number, email address or other information specific to that individual will be carried out. In each case, the scope of the search may be different.

10.4 If information is not part of a structured filing system, it does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

10.5 To be a structured filing system, the system must:

10.5.1 Contain information relating in some way to individuals. Usually, there would be more than one file in the system or a group of information referenced by a common theme (e.g. an absence spreadsheet). The files need not be located in the same geographical location, but could be dispersed over different locations;

10.5.2 be structured by reference to individuals (e.g. by name or employee or account number) or by reference to information relating to individuals (e.g. type of job or location, address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held;

10.5.3 be structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced to easily indicate whether and where in the file data about the individual is located.

10.6 Therefore, a structured filing system, which is subject to the data protection laws, must have an external and internal structure, which allows personal data about an individual to be located relatively easily without having to conduct a manual search of the entire file. If you have to thumb through the whole file to find specific information, the file is not a structured filing system.

10.7 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"), the GDPR Compliance Manager 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. However, it should be noted that it is entirely valid to make a request for all personal data, and therefore even with such a request we would need to comply. Therefore, if requesting and waiting for clarification, do not delay in conducting searches to locate personal data.

10.8 The GDPR Compliance Manager and People, Learning and Development department 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 The GDPR Compliance Manager or People, learning and Development department must respond to data subject requests no later than one month after receiving the request unless an exception applies.

11.2 If the GDPR Compliance Manager determines that a data subject request may take longer than one month to respond to, they will notify any relevant director or head of department via email. The GDPR Compliance Manager will determine if we can extend the one-month response time.

11.3 If we extend the period for responding to the data subject request the GDPR Compliance Manager or People, Learning and Development department must inform the data subject within one month of receipt of the request of the extension and explain the reason(s) for the delay. However if an extension is needed, and can apply, it is preferable to let the data subject know straight away rather than wait until the end of the month.

12. **GENERAL REASONS FOR DENYING A DATA SUBJECT REQUEST**

12.1 The People, Learning and Development department and GDPR Compliance Manager must determine if we have a basis not to respond to a data subject request. We may refuse to respond to data subject requests for the following reasons:

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

12.1.2 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.

12.1.3 National law provides a basis for denying the request.

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

12.1.5 We do not hold any personal data related to the data subject request but we would still have to respond to them to confirm this fact.

12.1 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 20. There may also be grounds to limit the scope of the request.

12.2 Where we refuse to respond to a data subject request, the GDPR Compliance Manager or People, Learning and Development department 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). They must also advise them of their right to complain to the supervisory authority and seek a judicial remedy.

12.3 If we do not have or process personal data related to the data subject, the GDPR Compliance Manager or People, Learning and Development department should indicate that we conducted a diligent search for records related to the data subject's request and did not uncover responsive results. The GDPR Compliance Manager or People, Learning and Development department should retain internal documents that show the steps we took to locate relevant personal data, including all the search methods used.

13. **FEES FOR RESPONDING TO DATA SUBJECT REQUESTS**

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

13.2 The GDPR Compliance Manager or People, Learning and Development department must determine whether we can charge a fee and the amount and then advise data subjects of that fee. The GDPR Compliance Manager or People, Learning and Development department must document the reasons for charging the fee. There may also be limits applied to the amount of the fee that can be charged.

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, the GDPR Compliance Manager or People, Learning and Development department must, unless an exemption applies under Paragraphs 12 and 14.5, provide data subjects with the following information about our personal data processing activities:

14.2.1 The purposes of processing.

14.2.2 Categories of personal data processed.

14.2.3 Recipients or categories of recipients who receive personal data from us.

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

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

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

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

14.2.8 Their right to:

(a) request correction or erasure of their personal data;

(b) restrict or object to certain types of processing with respect to their personal data; and

(c) make a complaint with the local data protection authority.

14.3 The GDPR Compliance Manager or People, Learning and Development department 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:

14.4.1 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.

14.4.2 Where the data set includes third parties' personal data, we must identify a legal basis under the GDPR prior to transferring the third parties' data. The People, Learning and Development department must determine whether we have a basis to transfer the third parties' data.

14.4.3 In cases where the People, Learning and Development department determine that we do not have a basis to transfer the personal data of third parties, the People, Learning and Development department may give instructions to redact or remove the personal data of the third parties 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 We do not have to disclose any personal data that is legally privileged. The following would be legally privileged:

14.6.1 confidential communications between us and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice; and

14.6.2 confidential communications between us or our lawyers and a third party (e.g. a witness) where the dominant purpose of the communication is to give or seek legal advice in respect of current or potential legal proceedings. This claim to legal privilege would end as soon as the case has been decided and, at that moment, the documents in the file might be disclosable if a subject access request is received.

14.7 We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

14.8 The People, Learning and Development department must determine if we have a basis not to respond to a data subject access request. The People, Learning and Development department 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.

14.9 We may charge a reasonable fee if data subjects request additional copies of their data. People, Learning and Development department must determine whether we can assess a fee and the amount and advise data subjects 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, the GDPR Compliance Manager must ensure that the personal data is rectified without undue delay unless a basis exists under Paragraph 12 to deny the request.

15.3 The GDPR Compliance Manager or People learning and Development department must identify each third-party recipient of the personal data that is the subject of the rectification request by e-mail. The GDPR Compliance Manager or People, Learning and Development department 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 GDPR Compliance Manager or People, Learning and Development issues a written finding that it is impossible or involves disproportionate effort. The GDPR Compliance Manager or People, Learning and Development must also inform the data subject about those recipients if the data subject requests it.

15.4 The GDPR Compliance Manager or People, Learning and Development must determine if we have a basis not to respond to the rectification request. The GDPR Compliance Manager or People, Learning and Development 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 us erase their personal data. Where such a request is made, The GDPR Compliance Manager or People, Learning and Development must, unless an exemption applies under Paragraphs 12 and 16.4, erase the personal data that is the subject of the request through deletion of information from systems and destruction of paper-based information if:

16.1.1 The personal data is no longer necessary for the purpose we collected it for.

16.1.2 The data subject withdrew his or her consent to our processing activities and no other legal justification for processing applies.

16.1.3 The data subject objects under GDPR Article 21(1) to:

(a) processing, including profiling, that is necessary for us to perform a task in the public interest or in the exercise of our official authority; and

(b) there are no overriding legitimate grounds to process the personal data.

16.1.4 The data subject objects under GDPR Article 21(1) to:

(a) processing, including profiling, that is necessary to pursue our or a third party's legitimate interests; and

(b) there are no overriding legitimate grounds to process the personal data.

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

16.1.6 We unlawfully processed the data subject's personal data.

16.1.7 EU or member state law requires us to erase the personal data to comply with a legal obligation.

16.1.8 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, the GDPR Compliance Manager or People, Learning and Development department 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, the GDPR Compliance Manager or People, Learning and Development department must identify each recipient to whom we disclosed the personal data that is the subject of the erasure request by email or letter. The GDPR Compliance Manager or People, Learning and Development department must communicate the erasure of personal data to the third-party data recipients, unless the GDPR Compliance Manager or People, Learning and Development department issues a written finding that this is impossible or involves disproportionate effort. The GDPR Compliance Manager or People, Learning and Development department 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:

16.4.1 The purpose of performing a contract or agreement with the data subject.

16.4.2 Exercising the right of freedom of expression and information.

16.4.3 Complying with a legal obligation under EU or member state law.

16.4.4 The performance of a task carried out in the public interest.

16.4.5 Exercising our official authority.

16.4.6 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).

16.4.7 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.

16.4.8 The establishment, exercise, or defence of legal claims.

16.5 The GDPR Compliance Manager or People, Learning and Development department must determine if we have a basis not to respond to a data subject erasure request. The GDPR Compliance Manager or People, Learning and Development department 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, the GDPR Compliance Manager or People, Learning and Development department must, unless an exemption under applies under Paragraph 12, restrict processing of the data subject's personal information if:

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

17.1.2 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.

17.1.3 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.

17.1.4 A data subject objects to processing, including profiling, for:

(a) purposes that we consider necessary to perform a task in the public interest; or

(b) 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 17.1 (d)(i) or 17.1 (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 as long as the right applies.

17.3 The GDPR Compliance Manager or People, Learning and Development department must determine if we have a basis not to respond to the data processing restriction request. The GDPR Compliance Manager or People, Learning and Development department 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, the GDPR Compliance Manager or People, Learning and Development department must ensure that we only process the personal data (excluding storing it) either:

17.4.1 For contractual performance.

17.4.2 With the data subject's consent.

17.4.3 For the establishment, exercise, or defence of legal claims.

17.4.4 For the protection of the rights of another person.

17.4.5 For reasons of important public interest.

17.5 The GDPR Compliance Manager or People, Learning and Development department must inform the data subject that we intend to lift the restriction seven days before lifting the restriction. We may lift the processing restriction when:

17.5.1 The GDPR Compliance Manager or People, Learning and Development department verifies the accuracy of the personal data that is the subject of the processing restriction request.

17.5.2 The GDPR Compliance Manager or People, Learning and Development department determines that our or a third party's legitimate interests override the data subject's interests if a data subject objects under Paragraphs 17.1(d)(i) or 17.1(d)(ii).

17.6 Where processing has been restricted, the GDPR Compliance Manager or People, Learning and Development department must identify each recipient to whom we disclosed the personal data that is the subject of the processing restriction request by email or letter. The GDPR Compliance Manager or People, Learning and Development department must communicate the processing restriction to the third-party data recipients, unless the GDPR Compliance Manager or People, Learning and Development department issues a written finding that it is impossible or involves disproportionate effort. The GDPR Compliance Manager or People, Learning and Development department 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:

18.1.1 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.

18.1.2 Transmit certain personal data to another data controller.

18.1.3 Have us 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:

18.2.1 Based on the data subject's consent; or

18.2.2 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 Millennium Point such as name, contact information, and browsing history. 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 GDPR Compliance Manager.

18.4 For personal data that the data subject requests be transmitted to a third party, the GDPR Compliance Manager or People, Learning and Development department must, unless an exemption applies under Paragraphs 12 and 18.7, transfer the personal data that is the subject of the data portability request by e-mail. However, if the data subject requests a particular format, the GDPR Compliance Manager or People, Learning and Development department should make efforts to transfer the data in that format.

18.5 For portability requests asking that the personal data be transmitted directly to the data subject, the GDPR Compliance Manager or People, Learning and Development department must, unless an exemption applies under Paragraphs 12 and 18.7 transfer the personal data that is the subject of the data portability request by e-mail. However, if the data subject requests a particular format, the GDPR Compliance Manager or People, Learning and Development department should make efforts to transfer the data in that format.

18.6 Personal Data Pertaining to Third Parties:

18.6.1 Where the data set includes third parties' personal data, we must identify a legal basis under the GDPR prior to transferring the third parties' data. The GDPR Compliance Manager or People, Learning and Development department must determine whether we have a basis to transfer the third parties' data. Usually we will not have such a basis.

18.6.2 In cases where our legal adviser determines that we do not have a basis to transfer the personal data of third parties, the GDPR Compliance Manager may give instructions to redact or remove the personal data of the third parties 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 GDPR Compliance Manager must determine if we have a basis not to respond to a data portability request. The GDPR Compliance Manager or People, Learning and Development department 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 OBJECTIONS TO PERSONAL DATA PROCESSING**

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

19.1.1 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.

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

19.1.3 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).

19.2 The GDPR Compliance Manager or People, Learning and Development department must, unless an exemption applies under Paragraphs 12 and 19.3 stop the personal data processing related to the data subject's request through removal from electronic systems or destruction of paper records.

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

19.3.1 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.

19.3.2 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:

(a) a compelling legitimate ground for processing the personal data that overrides the data subject's interests; or

(b) that we need to process the personal data to establish, exercise, or defend legal claims.

19.4 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.

19.5 If the GDPR Compliance Manager or People, Learning and Development department determines that there are no overriding legitimate grounds for the personal data processing under Paragraph 19.3(b), the GDPR Compliance Manager or People, Learning and Development must ensure that personal data is erased in accordance with Paragraph 16.

19.6 The GDPR Compliance Manager or People, Learning and Development department must determine if we have a basis not to respond to a data subject objection request. The GDPR Compliance Manager or People, Learning and Development department 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.

20. TRAINING AND AWARENESS

20.1 This policy will be published on the Millennium Point's website. The GDPR Compliance Manager or People, Learning and Development department will ensure that all staff subject to the Policy understand their roles in implementing this Policy through providing all staff with a copy of the policy and providing any training that may be required. Directors of departments will be responsible for training their teams on the contents.

21. ENFORCEMENT

21.1 Violations of or actions contrary to this Policy may result in disciplinary action, in accordance with Millennium Point's information security policies and procedures and human resources policies. Please see the Employee Handbook and shared drive for details regarding Millennium Point's disciplinary process.

I, _____ (employee name), acknowledge that on _____ (date), I received and read a copy of Millennium Point's Policy on Handling data subject requests dated [5th March 2019] and understand that it is my responsibility to be familiar with and abide by its terms. I understand that the information in this Policy is intended to help Millennium Point's employees to work together to handle data subject requests under the GDPR.

_____
Signature

_____
Printed Name

1. Policy Control

This is a controlled document. Whilst this document may be printed, the electronic version located on the S: Drive will be the most up to date version and the controlled copy. Any printed copies of the document are not controlled.

Date of Issue:	05.03.19	**Next Review Date:**	05.09.2020
Version:	1.1	**Last Review Date:**	05.09.2019
Document Owner:	Vanessa Currie, Head of PLD		
Department:	People, Learning & Development		
Policy Approval Route			
Policy Ref. No.	**Policy Name**	**Approved By:**	**Date Approved:**
1.1	Policy on handling data subject requests.	A Vlahakis – Interim CEO JJ Mian – Interim Finance Director L Degg – Facilities Director R Delmore – Commercial Director	12.03.19 12.03.19 12.03.19 05.03.19

2. Amendments

Issue:	Policy Ref. No.:	Date:	Reason for Change:	Authorised by:
1.2	1.2	05.09.2019	Removal of GDPR (Internal) from Policy Approval Route Policy Name	Abbie Vlahakis **(Interim CEO)**