Luther Pendragon Data Protection Policy

1. Introduction

1.1 Luther Pendragon is registered at the Information Commissioner's Office (ICO) as a holder of data. All staff are reminded of our data protection principles and are trained on General Data Protection Regulation (GDPR), Data Protection Act, and the Privacy and Electronic Communications Regulations (PECR). We ensure that any data we do hold temporarily is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights; and
- kept safe and secure.

1.2 This personal information must be handled properly under the GDPR 2018 ("the Regulation"). The Regulation controls the way that we handle "personal data" that we collect in the course of carrying out our functions and gives certain rights to people whose personal data we may hold.

1.3 We consider that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. We fully appreciate the underlying principles of the Regulation and support and adhere to its provisions.

1.4 We are registered with the ICO to process personal data. We are named as a data controller under the register kept by the ICO in accordance with section 19 of the Regulation.

1.5 We will ensure that at least one of the following conditions are met before we process any personal data:

- the individual has consented to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation (other than one imposed by a contract);
- the processing is necessary to protect vital interests of the individual;
- the processing is necessary to carry out public functions e.g. administration of justice; or
- the processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual).

2. Individuals' rights

2.1 We will ensure that individuals are given their rights under the Regulation including:

- the right to obtain their personal information from us except in limited circumstances;
- the right to ask us not to process personal data where it causes substantial unwarranted damage to them or anyone else; and
- the right to claim compensation from us for damage and distress caused by any breach of the Regulation.

3. Legal requirements

3.1 While it is unlikely, Luther may be required to disclose user data by a court order or to comply with other legal requirements. We will use all reasonable endeavours to notify the user before we do so, unless we are legally restricted from doing so.

3.2 Luther shall not sell, rent, distribute or otherwise make user data commercially available to any third party, except as described above or with prior permission.

4. Communicating and implementing this Policy

4.1 We will ensure that:

- everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- there is someone with specific responsibility for data protection in the organisation;
- staff who handle personal information are appropriately supervised and trained;
- queries about handling personal information are promptly and courteously dealt with;
- people know how to access their own personal information;
- methods of handling personal information are regularly assessed and evaluated;
- any disclosure of personal data will be in compliance with approved procedures;
- we take all necessary steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure; and
- all contractors who are users of personal information supplied by Luther confirm that they will abide by the requirements of the Regulation with regard to information supplied by us.

4.2 Nick Ward is the Data Protection Officer (DPO) who has been appointed to lead on data protection for Luther. He is responsible for ensuring that the Policy is effectively implemented.

5. Action to be taken in the event of a data breach

5.1 A breach of this Policy would take place if personal data held by Luther was compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose.

5.2 Data security breaches should be reported immediately to the DPO (Nick Ward). The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, and how many people are involved. The DPO will keep a log of this information.

5.3 The DPO will initiate an investigation into the breach within 24 hours of it being discovered, where possible. The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, and if so who are the subjects and how many are involved. It will also consider the extent of the sensitivity of the data, and a risk assessment will be performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to the company.

5.4 The DPO will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment. Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

5.5 The CEO and Executive Chair will be notified by the DPO following a critical data breach involving large amounts of data, or a significant number of people whose personal data has been breached. They will make a decision to inform any external organisation, such as the police or other appropriate regulatory body. The DPO will inform the ICO of the extent of the breach. Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the DPO.

5.6 Once the breach is contained a thorough review of the event will be undertaken by the DPO, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

We seek continuous improvement of our performance so regularly monitor and update this policy on the basis of feedback from staff, clients, and other stakeholders.

Key contact for this policy: Nick Ward, Data Protection Officer
Last reviewed: February 2024