DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

UPDATED REPRIMAND

1. Introduction and Summary

1.1. The Information Commissioner (the "**Commissioner**") has decided to issue a Reprimand to the London Borough of Hackney ("**LBoH**") in accordance with Article 58(2)(b) of the UK General Data Protection Regulation ("**UK GDPR**")[1] in respect of infringements of the following parts of the UK GDPR:-

- Article 5(1)(f) – a failure to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Article 32(1) – a failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

1.2. This Reprimand sets out the circumstances of the infringement, the nature of the personal data involved and the reasons why a Reprimand is deemed to be the appropriate and proportionate regulatory sanction in this case.

1.3. The Commissioner sent a Notice of Intent to impose a Reprimand to LBoH on 15 June 2023 ("**NOI**"). LBoH submitted written representations to the Commissioner in response to the NOI on 8 September 2023 (the "**Initial Representations**"). Following consideration of those Initial Representations, the Commissioner sent a follow-up letter to LBoH on 19 December 2023 (the "**December Letter**"), clarifying the bases for the proposed enforcement action, and inviting further representations from LBoH. LBoH submitted its further written representations on 15 February 2024 (the "**Further Representations**").

[1] For the purposes of this Reprimand, the version of the GDPR that is applicable is the GDPR as transposed into and modified by UK law (that is to say, the "UK GDPR"): *Lipton v BA City Flyer Ltd* [2021] EWCA Civ 454; [2021] 1 WLR 2545. There is however no material difference for the purposes of this Reprimand between the GDPR and the UK GDPR. If and to the extent that the law applicable is the GDPR as originally enacted rather than the UK GDPR, then references to the UK GDPR are to be read as references to the corresponding provisions of the GDPR.

1.4. This Reprimand takes into account all the evidence and information obtained by the Commissioner in the course of its investigation, and LBoH's Initial Representations and Further Representations (collectively, the "**Representations**"). The Commissioner has carefully considered all of the matters raised by LBoH both in the course of the investigation and in its Representations, and where appropriate, makes specific reference to them in this Reprimand.

1.5. Having carefully considered all the evidence and those Representations, the Commissioner finds that LBoH has infringed Articles 5(1)(f) and 32(1)(b) UK GDPR for the reasons set out in this Reprimand. In summary:

- The Commissioner finds that LBoH employed inadequate patch management which resulted in LBoH failing to process personal data in a manner which ensured appropriate security of that personal data. This failure was contrary to the requirements of Articles 5(1)(f) and 32(1)(b) UK GDPR.

- The Commissioner finds that LBoH employed insufficient user account management which resulted in LBoH failing to process personal data in a manner which ensured appropriate security of that personal data. This failure was contrary to the requirements of Articles 5(1)(f) and 32(1)(b) UK GDPR.

1.6. The Commissioner's provisional findings as set out in the NOI and the December Letter had also made reference to potential failings in respect of LBoH's internal vulnerability scanning, contrary to the requirements of Articles 5(1)(f) and 32(1)(d) UK GDPR[2], and to potential failings in respect of LBoH's procedures for ensuring robust adherence to its firewall policies, contrary to the requirements of Articles 5(1)(f) and 32(1)(b) UK GDPR[3]. However, having taken into account the Representations made by LBoH in respect of its internal vulnerability scanning[4] and its firewall policies/procedures[5], these provisional findings are not maintained and form no part of the decision to impose this Reprimand.

1.7. When enforcement action was first being considered against LBoH, given the seriousness of the potential infringements identified, the Commissioner was initially minded to impose a monetary penalty. However, the Commissioner has given consideration to the Public Sector posture announced in June 2022, and to the full facts of this matter, which have included considering the immediate impact of the COVID-19 pandemic, and LBoH's robust response to the cyber-attack which involved significant engagement with the relevant agencies such as the National Crime Agency ("**NCA**"), National Cyber Security Centre ("**NCSC**") and the Metropolitan Police. The Commissioner has also given due regard to LBoH's transparent approach, both towards those relevant agencies and to the Commissioner's

[2] NOI, §§2.18 – 2.22; and the December Letter, §§2.33 – 2.45.

[3] NOI, §§2.23 – 2.28; and the December Letter, §§2.46 – 2.61.

[4] Initial Representations, §§6(8) – (11), 24 – 27; and Further Representations, §§3(3), 20 – 24.

[5] Initial Representations, §§6(12) – (13), 28; and Further Representations, §§3(4), 25 – 32.

own investigation, and its willingness to learn and to take steps to prevent future attacks. In light of these factors, and having fully considered the evidence collected and the Representations which have been made, the decision has been taken to proceed with this case as a Reprimand. The reasons for the Commissioner's conclusion that a Reprimand is an appropriate and proportionate action, having regard to the Regulatory Action Policy, are set out in full below.

1.8. This Reprimand replaces an earlier version which was served on LBoH on 3 May 2024. The changes made for the purpose of this updated Reprimand are clarificatory in nature only, and are made following a series of further submissions put forward by LBoH on 8 and 14 May 2024. The changes made have not altered the basis of the Commissioner's findings in any way.

2. Relevant Legal Framework

2.1. This Reprimand relates to LBoH's failure to comply with the requirements of Article 5(1)(f) of the UK GDPR and Article 32(1)(b) of the UK GDPR.

- **Article 5(1)(f) UK GDPR** states that:

  "*Personal data shall be […] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*"

- **Article 32(1) UK GDPR** states in material part that:

  "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

  […]

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

  […]

- **Article 32(2) UK GDPR** states in material part that:

  "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss,

alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

2.2. The Commissioner issues this Reprimand in accordance with Article 58(2)(b) UK GDPR which provides that the Commissioner has the corrective power "*to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation*".

2.3. In reaching the decision to impose a Reprimand in this case, the Commissioner has had regard to the Regulatory Action Policy, and to the Public Sector posture announced in June 2022.

3. Factual Background

3.1. LBoH is the local authority for the London Borough of Hackney, London.

3.2. As relevant to this incident, LBoH processes its data in line with the HMG Classification Scheme, processing data within the 'OFFICIAL' and 'OFFICIAL-SENSTIVE' classification label. The typical threat profile for the 'OFFICIAL' classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources including by competent individual hackers and the majority of criminal individuals and groups.

3.3. LBoH became aware on 11 October 2020 of a "Pysa" ransomware attack which affected its access to personal data held on its internal systems/servers (the "**Attack**"). During the Attack, the malicious actor (the "**Attacker**") was able to access and encrypt the personal data, including special category data[6], contained within 440,000 individual files across a range of systems, relating to not less than 280,000 LBoH residents and other individuals including LBoH staff. The Attack affected LBoH's ability to maintain the timely access to personal data stored within its servers, with this loss of availability being due to either, or a combination of, encryption of the personal data processed; encryption of the host operating systems; or the system being taken offline as part of the immediate incident response containment.

3.4. The affected named systems included: [redacted].

3.5. The encryption affected personal data including, but not limited to, data revealing racial or ethnic origin, religious beliefs, sexual orientation, health

[6] As defined at Article 9(1) UK GDPR.

data, economic data, criminal offence data[7], and other data including basic personal identifiers[8].

3.6. Following an internal investigation, LBoH was able to determine that on 22 September 2020, the Attacker had gained access to the LBoH network via an open Remote Desktop Protocol ("**RDP**") port. The RDP port was opened on the perimeter firewall by a network engineer, operating outside of LBoH's policies, thereby allowing the Attacker to use the RDP port to access the engineer's device (the "**Device**") remotely via the internet. The Attacker then authenticated into LBoH's network using legitimate account credentials, likely via credential stuffing.

3.7. Accessing a network via the organisation's external remote services and using a compromised account via methods such as credential stuffing are tactics which are documented in the Mitre Attack Framework[9].

3.8. The account which the Attacker gained access to had previously been used as a public access account for a 'kiosk' device created in 2005, but had lain dormant since 2012 (the "**Account**"). Since its creation, and at the time of its exploitation, the username and password of the Account were both 'kiosk'. At the time of the Attack, as a dormant account, the Account should have already been disabled, however, for unknown reasons, it had been

[7] As defined at Article 10 UK GDPR as "personal data relating to criminal convictions and offences or related security measures".

[8] Across the various systems, the affected data included: [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [for [redacted]] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted]; [For '[redacted]'] [redacted].

[9] The Mitre Framework is a globally accessible knowledge base of known adversary tactics and techniques based on real-work observations.

incorrectly labelled as a 'service account' and excluded from automated disabling. No manual steps had been taken to disable the Account.

3.9. On 2 October 2020, and once authenticated to the Device, the Attacker identified a known vulnerability within the Microsoft operating system: CVE-2020-0787. This was an 'elevation of privileges' vulnerability which allowed the Attacker to log onto the LBoH system using a 'standard' user account and then elevate its status to a 'privileged' account. This method of privilege escalation is documented in the Mitre Attack Framework.

3.10. The CVE-2020-0787 vulnerability had previously been given a 'base score' by the CVSS as '7.8', indicating that it was a "high" risk vulnerability[10], although it is acknowledged that Microsoft had identified the vulnerability as "Exploitation Less Likely"[11]. A patch to fix this vulnerability was released by Microsoft on 10 March 2020, along with related security guidance. However, as explained below, the patch had not been applied to the Device because the Device had been omitted from LBoH's patch management software.

3.11. On 11 October 2020, with the elevated privileges, the Attacker was able to access servers and devices within the LBoH network, execute the Attack and encrypt data. The encryption of data is a known attack method documented in the Mitre Attack Framework. The Attacker was also able to exfiltrate data from the network.

3.12. The encryption spread to LBoH's on-premises environment including approximately 125 servers hosting Microsoft server operating systems, and approximately 1,000 VDI desktop instances hosting Microsoft client operating systems.

3.13. On the same date, the Attacker also accessed the LBoH's backup and initiated a deletion process of the data on the disk. The deletion process was identified by the engineers responding to the Attack and interrupted when the deletion was in progress and was 10% complete. The targeting and deleting of backups are documented in the Mitre Attack Framework.

3.14. Upon becoming aware of the issue, LBoH took steps on 11 October 2020 to isolate its network from the internet, thereby removing the threat of further exploitation of its systems[12].

3.15. On 6 January 2021, LBoH was notified by the NCA that a collection of data which had been exfiltrated as part of the Attack had been published onto the "dark web" via an '.Onion' site[13]. Due to the nature of the site, LBoH was unable to remove the published data. This published data is known to

[10] The CVSS is an industry standard rating of software vulnerabilities. Its takes into considerations all the factors of the vulnerability and provides a score in relation to the risk.

[11] CVE-2020-0787 - Security Update Guide - Microsoft - Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability

[12] §7 of this Reprimand set out the additional remedial steps taken by LBoH following the Attack.

[13] An Onion site is a website on the dark web which is designed to offer anonymous services over the Tor network and are only accessible with dark web browsers such as the Tor browser.

have consisted of [redacted][14].

3.16. LBoH has since confirmed that the exfiltrated data comprised approximately 9,605 personal data records[15], with the Attack being acknowledged by LBoH to have "*posed a meaningful risk of harm to [...] 230 data subjects*"[16].

4. Contents of this Reprimand

4.1. The following sections of the Reprimand set out the bases on which the Commissioner has determined that LBoH has contravened the UK GDPR and the reasons for those conclusions. This Reprimand then sets out the reasons why the Commissioner has concluded that a Reprimand is an appropriate and proportionate sanction.

4.2. Each 'Infringement Finding' at §§5 and 6 below includes detail of the context for the finding (a 'background'); details of the relevant Representations made by LBoH; and the Commissioner's findings and reasons for those conclusions, having taken account of all the evidence and the Representations.

4.3. The Infringement Findings are followed, at §7, by the Commissioner's consideration of the remedial steps taken by LBoH since the time of the infringement.

4.4. The Reprimand, from §8, provides an explanation of the Commissioner's broad discretion to impose a Reprimand, including consideration of the relevant criteria set out within the Regulatory Action Policy[17]. This section also assesses LBoH's various Representations on the issue of regulatory discretion (from §8.17), before ending with a short conclusion on the regulatory action taken at §9.

5. Infringement Finding 1 - Inadequate Patch Management (Article 5(1)(f) and 32(1)(b) UK GDPR)

i) Background

5.1. In 2018, LBoH sought to replace its 'Windows Security Update Services' patch management system ("**WSUS**") with [redacted] ("[redacted]"), a state-of-the-art patching system in respect of Windows devices.

5.2. At the time of the Attack, LBoH had commenced (but not completed) an extensive program to reduce its use of Windows-based devices, in order to reduce Windows-related vulnerabilities.

[14] Further information on the published data is provided at §8.4 of this Reprimand.
[15] Initial Representations, §35(2), Further Representations, §34(2)(i).
[16] Initial Representations, §35(3).
[17] Regulatory Action Policy (ico.org.uk)

5.3. A vulnerability in relation to Windows devices known as CVE-2020-0787, which enabled the elevation of privileges, was identified by Microsoft and a patch was released for this on 10 March 2020.

5.4. LBoH's [redacted] system sought to apply this patch to all of the Windows devices on its system in March 2020. However, the patch was not applied to the Device. The reason for that is that whilst the Device had been registered with LBoH's asset management system ("[redacted]") and registered with its previous patch management system, WSUS, the Device was not added to the [redacted] system, and therefore patches were not deployed to it.

5.5. It is understood that this was an omission by the infrastructure team working to implement the [redacted] system and this omission was not identified in the review of the proposed change, or at any point thereafter. Therefore, the CVE-2020-0787 vulnerability in respect of this Device remained on 2 October 2020, when this was exploited by the Attacker to elevate the standard user account to a privileged account.

5.6. Had the relevant patch been applied to the Device, the Commissioner is satisfied that it would have prevented the Attacker from gaining privileged access via this route, and ultimately from being able to access, encrypt, and exfiltrate data.

ii) <u>Representations</u>

5.7. LBoH made detailed Representations in relation to the Commissioner's provisional findings regarding this infringement as they were outlined in the NOI[18] and the December Letter[19]. These have been carefully considered by the Commissioner in full, and can be summarised as follows:

5.8. Initial Representations:[20]:

5.8.1. [redacted] was a robust, state-of-the-art automated system which did promptly patch the identified vulnerability;

5.8.2. The Device was not migrated to [redacted] because of "human error", rather than a failure by LBoH to apply appropriate security measures, and this is no basis for concluding that LBoH failed to have in place appropriate security measures;

5.8.3. The CVE-2020-0787 vulnerability itself had been identified by Microsoft as a lower category of vulnerability and therefore did not require urgent patching.

[18] NOI, §§2.2 – 2.9.

[19] The December Letter, §§2.3 – 2.20.

[20] Initial Representations, §§6(1) – (5), 16 – 19.

5.9. Further Representations:[21]:

5.9.1. LBoH suggest that the Commissioner has misapplied the security duty as if it imposed strict liability on LBoH (i.e. to ensure a particular outcome rather than to have appropriate processes);

5.9.2. LBoH did have appropriate measures for the purpose of ensuring that its patching system was effective, namely its Change Control Process ("**CCP**") (referred to previously within LBoH's Representations and interchangeably as its 'Change Management Process');

5.9.3. To require a further system beyond the CCP would be disproportionate when Windows devices (of which the Device was one) were only a small proportion of the estate and where Microsoft had categorised the vulnerability as relatively low risk;

5.9.4. The Commissioner's reliance on various assorted 'industry standards' take it no further.

iii) <u>The Commissioner's Findings and Conclusions</u>

<u>Summary of Findings</u>

5.10. The Commissioner's findings in relation to this infringement can be broadly summarised as follows and are expanded upon from §5.11 onwards:

5.10.1. LBoH did not have in place appropriate policies or processes to account for all relevant devices either as part of the transition from WSUS to [redacted], or thereafter, in order to address the need for the patch management system to be applied to all relevant devices – including the Device.

5.10.2. The discharge of the security duty in this context required LBoH to have both an adequate patch management system (i.e. software) and also to have adequate and effective policies and processes in place to apply that software to all relevant devices on its network.

5.10.3. LBoH has failed to provide evidence of adequate assurance controls to address the need for all relevant assets to be accounted for within [redacted], both at the point of the transition and thereafter.

5.10.4. Notwithstanding the risks of human error in the transition process, there was no evidence of appropriate systems or processes to identify or remediate these risks.

5.10.5. LBoH has failed to demonstrate that it had appropriate policies or processes in place to apply its patch management system to all relevant Windows devices and to address the risk that all relevant

[21] Further Representations, §§3(1); 4 – 15.

devices were accounted for, and therefore this error occurred as a result of deficient technical and organisational measures.

5.10.6. Accordingly the Commissioner is satisfied that LBoH failed to implement appropriate measures to address the need for the patch management system to be applied to all relevant devices and to address the need for [redacted] to be applied to all Windows devices on its system, both at the time of the system transition and thereafter, and this failure constitutes an infringement of Articles 5(1)(f) and 32(1)(b) UK GDPR.

Further Detail Regarding Findings

5.11. Having considered the evidence provided by LBoH throughout this case, including the Representations, the Commissioner's conclusions in relation to the findings outlined at §5.10 will be elaborated upon further below.

5.12. The Commissioner's findings are not that the [redacted] system (or its preceding WSUS system) was itself deficient, but rather that LBoH's patch management system was not effectively applied to all Windows devices on its network as it should have been, either at the time of the system transition or thereafter[22].

5.13. The Commissioner has taken account of the fact that [redacted] was not applied to all relevant devices within LBoH's network, nor did LBoH have in place appropriate policies or processes to account for all relevant devices as part of the transition to [redacted], or thereafter, in order to address the need for the patch management system to be applied (or to have been applied) to all relevant devices.

5.14. In the Commissioner's view, the requirement to take steps to apply an appropriate patch management system to all devices on a network is an integral part of the obligations to put in place a patch management system that addresses the security risk of having devices on a network which may have vulnerabilities. Specifically, the discharge of the security duty in this context would require LBoH to have both an adequate patch management system and also to address the need for it to be effectively applied to all devices on its network to address the risk and, in the latter respect, to put in place appropriate policies and processes to satisfy the need for the software to be applied to all relevant devices.

5.15. LBoH has suggested in its Further Representations that the Commissioner is adopting a strict liability approach, i.e. that it has not focussed on the duty of LBoH to have appropriate processes, but has focussed instead on the outcome[23]. However, the Commissioner's expectations of LBoH align with the obligations set out in the UK GDPR, which is to ask the question of whether, taking account of relevant matters (including industry standards, cost, and risk), LBoH had in place appropriate measures to address the risk

[22] NOI, §2.4; the December Letter, §2.3.

[23] Further Representations, §§3(1), 6.

of software vulnerabilities through an effective patch management system. Whilst it is common ground that the software itself was adequate, the pertinent issue is whether LBoH had in place adequate policies and processes to address the application of that software to all relevant devices on its network. For the reasons explained within this Reprimand, the Commissioner finds that it did not.

5.16. In its Further Representations, LBoH has drawn reference to its CCP which it says demonstrates that it did indeed have appropriate measures for the purpose of ensuring that its patching system was effective[24]. LBoH has been unable to provide a copy of the CCP as it was impacted by the Attack, however it has previously provided a description of that CCP during the Commissioner's Investigation[25]. This description purports to set out a process for making changes to LBoH's IT environment, and the Further Representations also state that there was a specific officer responsible for ensuring all assets were under the control of the patch management system[26].

5.17. The Commissioner has considered these Representations, however it is considered that the CCP as described is limited and far too generic to adequately or effectively ensure appropriate patch management across LBoH's network. The Commissioner takes the view that a further policy or process would be needed to adequately and effectively address the application of the [redacted] software to Windows devices on the network and to conduct appropriate auditing of the assets on the patch management system, such as by way of an appropriate asset management register, and via appropriate event management[27].

5.18. In the Commissioner's view, the security duty under Articles 5(1)(f) and 32(1)(b) required LBoH, as a data controller in respect of large quantities of personal data, including special category data, to do more to address the risk of software vulnerabilities on its devices than have a general CCP which applied to any proposed changes to its IT environment. Indeed, the risks arising from an IT system with inadequate patch management through omission of particular devices is so significant that further measures beyond the general CCP, and the documents provided, were needed to address the risk that not all relevant assets were subject to patch management software.

5.19. It is noted that LBoH have cited the fact that the "vast majority" of its end-user devices were [redacted] devices, rather than Windows devices, and since [redacted] is a Windows-only solution, it would be a disproportionate

[24] Further Representations, §§3(1), 10 – 11.

[25] LBoH letter to ICO, 22 January 2021.

[26] Further Representations, §9.

[27] LBoH has pointed to a range of documents which it says provide details of its patching management implementation and audit measures, specifically: a patch management procedure describing the steps to deploy patches, a server build process including details of deploying patches, a patch schedule and patch status reports. However, in the Commissioner's view these measures (which primarily address the deployment of patches) do not demonstrate that appropriate measures were in place to ensure that the whole network was accounted for in [redacted].

application of the security duty to require LBoH to implement measures to prevent all possible human error[28] where the devices represented a very small proportion of LBoH's estate. However, the Commissioner takes the view that even if the Windows devices were in a minority, (because the vast majority in use were [redacted] devices), they were still devices on the LBOH estate which posed a significant security risk if not subject to appropriate patch management software, and if the number of these devices were limited the extent of any auditing would have not been burdensome.

5.20. The Commissioner has concluded that LBoH should have had in place policies and/or processes to account for all relevant devices as part of the transition from WSUS to [redacted], and thereafter, in order to address the need for the patch management system to be actively applied to all devices – including its Windows devices. This might include:

- Collecting relevant server information regularly for vulnerability management purposes;
- Conducting asset management testing to be able to detect unauthorised devices or non-compliant software configurations;
- Using active and passive discovery tools to identify all assets connected to the network;
- Establishing and maintaining a detailed asset inventory to manage vulnerabilities.

5.21. The measures which the Commissioner contemplates should have been in place include processes and policies addressing the application of appropriate software to all of LBoH's devices, including processes for checking or auditing the application of the software to all relevant devices at the point of transition and at regular intervals, and a process for evaluating any changes.

5.22. Whilst LBoH appears to acknowledge that human error is "unavoidable"[29] (and hence foreseeable), the Commissioner notes that there is little evidence that it had deployed appropriate systems or processes to identify and remediate these risks across its whole estate.

5.23. Although [redacted] was applied to those assets which LBoH had identified, it was not applied to those assets which had not been identified but remained connected to LBoH's network. The Commissioner takes the view that, as a matter of principle, it cannot be correct that an organisation can discharge its security duty by implementing a patch management system on only some of its devices. An effective approach to patching vulnerability must require a combination of both effective software and effective application or implementation of that software to all devices which are connected and

[28] Further Representations, §12.
[29] Initial Representations, §14(6).

therefore pose a potential risk to the security network if they have identified vulnerabilities. Whilst LBoH had effective software, i.e. [redacted], it did not effectively apply it, or have adequate policies or processes in place to address the need for the software to be applied to all Windows devices on its network, either at the time of the system transition or thereafter.

5.24. Had the relevant patch been appropriately applied to the Device, the Commissioner is satisfied that it would have prevented the Attacker from being able to exploit the vulnerability to gain privileged access. This does not appear to be disputed by LBoH.

5.25. LBoH have provided no specific evidence of assurance controls to check whether all relevant connected assets were accounted for in [redacted]. In the Commissioner's view, the issues identified point to systemic rather than individual human failures.

5.26. In terms of the Commissioner's reference to the CVSS's categorisation of CVE-2020-0787 as a 'high" risk vulnerability, the Representations conversely draw attention to the categorisation of CVE-2020-0787 by Microsoft as a lower category vulnerability[30]. The Commissioner would note that this vulnerability allowed the Attacker to gain access, encrypt and exfiltrate thousands of data subjects' data, some of which was special category data. Therefore, despite the variance in classification, it was a significant risk which required appropriate patching across any devices which could be used to access that data.

5.27. Furthermore, the fact that the particular vulnerability which was exploited in the Attack was, on LBoH's case, at the lower end of risk, does not answer the point that adequate processes should have been in place to address any software vulnerabilities (whether high or low threat), which presumably may in any event not be apparent until a patch is released and categorised by the software manufacturer on release.

5.28. In making a finding that LBoH has fallen short of its duties under Articles 5(1)(f) and 32 UK GDPR, the Commissioner has considered the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Taking these points in turn:

State of the art

5.29. The Commissioner considers that these failures are contrary to major industry standards, including:

- The Commissioner's/NCSC's Security Outcomes guidance[31] recommends actively managing software vulnerabilities, including using in-support software and the application of

[30] Initial Representations, §16(2).

[31] GDPR security outcomes - NCSC.GOV.UK

software update policies (patches) and taking other mitigating steps, where patches cannot be applied.

- The Cabinet Office's Minimum Cyber Security Standard[32] in place at the time of the Attack required that organisations ensure that any infrastructure is not vulnerable to common cyber-attacks. It stated that this should be through secure configuration and patching.

(The following guidance post-dates the Attack, however it serves to demonstrate the continuing importance of appropriate patch and asset management.)

- NCSC Guidance Re: Asset Management[33]:

  "*[When designing an asset management system] It may be appropriate to collect server information once a week because changes are infrequent, but desktop information may be needed once a day for configuration accounting or vulnerability management*".

- NCSC Guidance Re: 10 Steps to Asset Management[34]:

  "Have a plan to validate your asset management system. For example, you should test your system to ensure unauthorised devices or non-compliant software configurations can be detected. This validation helps ensure that your understanding of your systems and data is accurate and therefore that you are not exposed to unidentified risks".

- CIS Critical Security Controls[35]:

  "***Control 01: Inventory and Control of Enterprise Assets / 1.3 Utilize an Active Discovery Tool*** *- Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently* ***/ 1.5 Use a Passive Asset Discovery Tool*** *- Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently".*

[32] The Minimum Cyber Security Standard - GOV.UK (www.gov.uk) – This guidance was withdrawn on 3 July 2023 but was in force at the time of the Attack.
[33] Asset management - NCSC.GOV.UK
[34] 10 Steps to Cyber Security - NCSC.GOV.UK
[35] learn.cisecurity.org/CIS-Controls-v8-guide-pdf

- 'International Organisation for Standardisation' Guidance, ISO/27002:2022[36], specifically:

  '5.9 - Inventory of information and other associated assets'

  > *"The organization should identify its information and other associated assets and determine their importance in terms of information security. Documentation should be maintained in dedicated or existing inventories as appropriate. […] The inventory of information and other associated assets should be accurate, up to date, consistent and aligned with other inventories".*

  '8.8 - Management of technical vulnerabilities'

  > *"The organization should have an accurate inventory of assets […] as a prerequisite for effective technical vulnerability management. […] To identify technical vulnerabilities, the organization should consider: a) defining and establishing the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, updating, asset tracking and any coordination responsibilities required.*
  >
  > *[…]*
  >
  > *An audit log should be kept for all steps undertaken in technical vulnerability management. The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency".*

- Furthermore, ISO/27002 also advises that organisations should define a timeline to react to notifications of potentially relevant technical vulnerabilities, and once a vulnerability has been identified, associated risks should be identified and actions taken, such as patching the system to remove the vulnerability.

5.30. These Standards emphasise the need to have appropriate asset management in place, and to have appropriate systems in place to ensure all assets within a network are appropriately secure and regularly updated.

5.31. LBoH relies heavily within its Representations on their stated compliance with the PSN Code of Connection (the "**PSN Code**") and NHS Toolkit[37]. As

[36] ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls

[37] Initial Representations, §18(5); and Further Representations, §14.

to compliance with the PSN Code, it is noted that the Gov.UK Guidance on PSN compliance expressly states that: "*PSN compliance is not a way to deliver security across your business*", and meeting the PSN requirements is not a "*substitute for engaging in ongoing risk assessment, management and mitigation across your business*"[38].

5.32. Therefore, the Commissioner's view is that whilst compliance with the PSN Code was the minimum standard expected in order to be authorised to access the PSN, compliance with the PSN Code alone is not necessarily sufficient to discharge UK GDPR obligations.

5.33. Furthermore, the PSN Code, on vulnerability management (patch management), emphasises the critical nature of timeliness in ensuring appropriate and thorough patching. Stating that: "*You must ensure that any exploitable vulnerability is managed. You must have a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities. Your policy will specify specific patch application periods and a process for auditing compliance*", noting that patches should be applied within no more than 60 days. It goes on to state that "*Where a patch is not deployed (or available) within the timescales above then there must be alternative mitigating action, such as disabling or reducing access to the vulnerable service*"[39]. Whilst LBoH did deploy the relevant patch across *some* of its network, it is evident that it was not deployed across *all* of its Windows devices as it should have been. Furthermore, there is no evidence of alternative mitigating action to protect the vulnerable service.

5.34. Similarly, the Commissioner's view of the NHS Data Security and Protection Toolkit is that it is something that organisations processing NHS data should use as a self-assessment tool to measure their performance against certain security standards, however it is not equivalent to the industry-wide standards cited by the Commissioner above.

Costs

5.35. The Commissioner takes the view that the costs of implementation would not have been a barrier in this instance, for the following reasons.

5.36. The patch itself was available at no cost, and was indeed already being implemented across some devices on LBoH's estate. LBoH did not require any new software or hardware that it had not already acquired and implemented successfully in respect of other areas of its network.

5.37. In terms of the cost of accounting for all relevant devices as part of the transition to [redacted], and thereafter, in order to satisfy itself that the patch management system was being applied to all relevant devices, the Commissioner concludes that – given the volume and nature of the data processed by LBoH - the risk posed by having vulnerable devices on the

[38] Public Services Network (PSN) compliance - GOV.UK (www.gov.uk)

[39] PSN_Code_of_Connection_v1.32.odt (live.com) (version 1.32 from September 2022)

network would justify the limited cost of implementing an appropriate system to ensure accurate asset management.

Nature, scope, context and purposes of processing

5.38. Given the volume and nature of LBoH's processing's activities, and the risks presented as a consequence of that processing, the Commissioner finds that it is not reasonable for LBoH to rely primarily on its general CCP as evidence of its efforts to implement and audit patch management compliance, particularly where that description is imprecise as to the particular issue.

Duration

5.39. In terms of the duration of this infringement, the relevant failure technically commenced from the point when LBoH migrated to [redacted] (and the Device was omitted from the migration) but, so far as this finding is causally relevant to the Attack, the breach occurred between 10 March 2020 (when the patch was released to address the vulnerability and should have applied to the Device) and 11 October 2020 (when the Device ceased to be in use and was isolated from the network).

Conclusion

5.40. For the above reasons, the Commissioner finds that LBoH failed to implement appropriate technical and organisational measures in order to ensure an appropriate level of security for the personal data which it processed. In particular, it failed to implement appropriate measures to address the need for the patch management system to be applied to all relevant Windows devices on its system, either at the time of the system transition or thereafter, and this failure constitutes an infringement of both Article 5(1)(f) and Article 32(1)(b) UK GDPR.

6. Infringement Finding 2 - User Account Management (Article 5(1)(f) and 32(1)(b) UK GDPR)

i) Background

6.1. The Account which was used to implement the Attack had previously been used as a public access account for a kiosk device, and had been created in 2005. The Account became dormant in 2012.

6.2. The username and password for the Account were both 'kiosk', and although it had been dormant for eight years, it remained connected and enabled on LBoH's network.

6.3. The Account should have been disabled, but it had not been because it had been incorrectly labelled as a 'service account' and therefore excluded from automated disabling. LBoH has not explained why the Account had been incorrectly labelled. Further, no other process or manual intervention was taken to audit whether those accounts which had been labelled as 'service

accounts' were active or needed to be disabled, or whether they complied with the minimum password standards.

6.4. A copy of a previous draft of LBoH's access control policy from 2012 prescribed a minimum password standard that the Account credentials ('kiosk') did not comply with[40].

6.5. Furthermore, because the Account had not been used to log-in since prior to the 2012 policy, there was no prompt to change the password to comply with the new policy.

6.6. In July 2019, LBoH commissioned an annual IT Health Check which reviewed the Active Directory and identified issues relating to password re-use and insufficient password strength on some privileged accounts. LBoH updated its Active Directory in an attempt to enforce minimum password standards on its system accounts, but this was ineffective in relation to 'service accounts' as these did not have their passwords updated manually and they remained non-compliant with the new policy.

6.7. The draft Audit Report provided to LBoH in April 2020 identified 1,525 accounts as being inactive or unused, including the Account, and identified issues relating to account management as "high risk".

6.8. LBoH did not review the draft Audit Report before the Attack, nor did it take steps to remove the unused or inactive accounts before the Attack. LBoH explained that it had de-prioritised the entirety of its Internal Audit from March 2020 when it was focussed on the response to the COVID-19 pandemic. This de-prioritisation included de-prioritising the consideration and implementation of the draft Audit Report.

ii) <u>Representations</u>

6.9. LBoH made detailed Representations in relation to the Commissioner's provisional findings regarding this infringement as they were outlined in the NOI[41] and the December Letter[42]. These have been carefully considered by the Commissioner in full, and can be summarised as follows:

6.10. Initial Representations:[43]:

6.10.1. LBoH has robust Mandatory Access Controls ("**MAC**") which require all accounts to have complex passwords with updates being applied automatically at the point of user sign-on and with auto-expire on unused accounts;

[40] The access control policy relevant to the investigation could not be provided because it had been encrypted by the Attack.
[41] NOI, §§2.10 – 2.17.
[42] The December Letter, §§2.24 – 2.31.
[43] Initial Representations, §§6(6) – (7), 20 – 23.

6.10.2. The reason the Account was not subject to these automated processes was that it was incorrectly treated as a 'service account', likely as a result of human error;

6.10.3. The IT Health Check conducted in July 2019 did not identify the non-compliant Account for reasons which are not known;

6.10.4. LBoH had processes in place to identify and remedy security weaknesses e.g. the draft Audit Report produced in April 2020 which identified the dormant Account;

6.10.5. The reason the Account was not de-activated is that the draft Audit Report was de-prioritised in light of the COVID-19 pandemic.

6.11. Further Representations:[44]:

6.11.1. LBoH had robust audit processes, including an IT Health Check carried out in 2019 (which detected issues with password non-compliance) and also the draft Audit Report in April 2020 which identified the Account as dormant;

6.11.2. The only reason this audit was not addressed sooner is that the COVID-19 pandemic intervened, meaning that it was not reasonably possible to progress the work more promptly;

6.11.3. The Commissioner cannot say that a stronger password wouldn't have been exploited by the Attacker;

6.11.4. In addition to password protection, LBOH uses multi-factor authentication ("**MFA**"). The Account should have been subject to MFA (but was not due to an error in the RDP port opening without requiring authentication) and therefore if the engineer had not made an error in opening up the port the password alone would have been insufficient to obtain access.

iii) <u>The Commissioner's Findings and Conclusions</u>

<u>Summary of Findings</u>

6.12. The Commissioner's findings in relation to this infringement can be broadly summarised as follows and are expanded upon from §6.13 onwards:

6.12.1. The findings in relation to user account management stem from two failings namely:

(i) the failure to implement appropriate measures to identify and disable dormant accounts and regularly review and audit access controls; and,

[44] Further Representations, §§3(2), 16 – 19.

(ii) the failure to implement appropriate measures to ensure the password policies were enforced in respect of all account types and audit compliance.

6.12.2. As to (i), there was no evidence of any process to regularly review and audit whether access rights on 'service accounts' remained appropriate (in particular taking account of the fact that automatic disabling measures were disapplied) and the draft Audit Report, which did identify the Account, was not even read until after the Attack.

6.12.3. As to (ii), there was no process in place to ensure LBoH's password policy was adhered to in practice and no process to ensure that accounts which did not have human users or were treated as 'service accounts' were compliant with the password policy or subject to manual updates, nor was there any effective audit system to ensure the accounts were compliant with its password policy.

6.12.4. The failure to have in place appropriate measures to identify/ audit all dormant accounts on LBoH's servers, and the failure to ensure that its password policy was enforced across its whole estate, constitutes a failure to implement appropriate technical and organisational measures in order to ensure appropriate security, in breach of Articles 5(1)(f) and Article 32(1)(b) UK GDPR.

Further Detail Regarding Findings

6.13. Having considered the evidence provided by LBoH throughout this case, including the Representations, the Commissioner's conclusions in relation to the findings outlined at §6.12 will be elaborated upon further below.

6.14. The Commissioner's findings in relation to LBoH's user account management stem from two critical failings.

6.15. Firstly, the failure to implement appropriate measures to identify and disable dormant accounts and regularly review and audit access controls.

6.16. In this case, the Attacker was able to exploit a dormant account which had been labelled as a 'service account', and which, following its creation in 2005, had been dormant since 2012.

6.17. For those accounts which were labelled as 'service accounts' (whether correctly or not) the Commissioner has seen no evidence that there was any process in place for reviewing whether access rights remained appropriate. Given that the automatic disabling provisions that were applicable to user accounts had been disabled for 'service accounts', in the Commissioner's view, there should reasonably have been an alternative process or policy for reviewing 'service accounts' to see if the access rights remained justified. It does not appear that there was any policy or process

which required consideration of whether the 'service accounts' required access to LBoH's systems[45].

6.18. Furthermore, there was no regular and effective auditing of whether access rights remained appropriate. Given that the relevant Account had been dormant since 2012, and this was not identified until Spring 2020[46], this is indicative of a failure to put in place processes for ensuring that all accounts were regularly and effectively audited and that dormant accounts were identified.

6.19. Regarding LBOH's reliance on its 'robust MAC policy'[47], it has been unable to provide a copy of the version relevant to the Commissioner's investigation due to it being encrypted in the Attack, however, there has evidently been a failure to sufficiently (and, crucially, regularly) review and audit access controls, as in excess of 1,500 accounts were found to be dormant in the April 2020 draft Audit Report. This casts significant doubt on how "robust" the MAC policy was, and in any event how effectively it was implemented by LBoH. The fact that the exploited Account had been dormant for eight years prior to discovery is further evidence of this.

6.20. Finally, the draft Audit Report which did finally identify the dormant Account – which was produced in April 2020 – was not acted upon promptly, and indeed does not appear to have been considered by LBoH until after the Attack had taken place, due to the relevant email attaching the Report being missed by the two responsible employees[48].

6.21. This draft Audit Report identified in excess of 1,500 inactive accounts, including the Account, prior to the Attack taking place in October 2020. The Audit had also identified that there were no processes to identify and disable inactive or unused accounts and a lack of audit policies[49] and set as high priority that these were promptly disabled. The Commissioner understands from LBoH's evidence that no-one read the draft Audit Report until after the Attack[50].

6.22. Whilst the circumstances of the pandemic constitute strong mitigating factors in terms of reacting to the 2020 draft Audit Report, not least given the demands on LBoH at the time[51], in light of the scale, volume and nature

[45] Contrary to the suggestion at §17(1) of the Further Representations, the Commissioner is not proposing to make a finding that the misclassification of the account is a relevant breach. Rather, that for those accounts which were labelled as 'service accounts' there does not seem to have been any policy or process for ensuring that the ongoing access rights were regularly reviewed and/or passwords were compliant.

[46] Having been missed in the IT Health Check conducted in July 2019, and having not been identified at any point since 2012.

[47] Further Representations, §17(1).

[48] Further Representations, §17(3)(iii).

[49] Cyber Resilience Audit (LBoH's letter to the Commissioner, 23 July 2021 – Appendix 10).

[50] The Representations suggest that the two recipient responsible officers missed the email attaching the draft Audit report "*in view of the enormous volume of emails they were receiving at the time, by virtue of their having been appointed into lead roles aimed at addressing the Covid pandemic*" (Initial Representations, §20(4)(b); see also Further Representations, §17(3).

[51] As set out in the Further Representations, §17(3).

of data being processed by LBoH, the Commissioner finds that it would be reasonable for LBoH to have had in place a more regular and robust auditing system which was capable of identifying dormant/vulnerable accounts far sooner than it did, without having to rely on the 2020 draft Audit Report to alert it to these significant security issues.

6.23. Indeed, whilst the Commissioner takes account of and is sympathetic to the considerable demands on LBoH during the COVID-19 pandemic which mitigates to some extent LBoH's delay in responding to the draft Audit Report produced in April 2020, it remains the case that by the time of the Attack there were 1,500+ inactive accounts which had gone undetected for an indeterminant amount of time, with the compromised Account itself being dormant for eight years. In that time, there were demonstrably insufficient procedures in place for auditing and remedying all inactive (and potentially vulnerable) accounts on the network, including no appropriate checks and periodic reviews to ensure that its technical system permissions were consistent with its documented user access rights.

6.24. The fact that the Account was finally identified in April 2020 and that LBoH was delayed in remedying this in a timely fashion because of the demands of the pandemic is a factor in the Commissioner's decision-making, but the demands of the pandemic do not account for the considerable amount of time prior to 2020 where the Account could (and – in the Commissioner's view - reasonably should) have been identified and remedied, particularly following the implementation of GDPR in 2018.

6.25. The Commissioner believes that had the compromised Account been identified by LBoH as dormant prior to the Attack, it could have been decommissioned and would not have been capable of being exploited to gain unauthorised access to LBoH's servers.

6.26. The second failure involves the failure to implement appropriate measures to ensure the password policy was enforced in respect of all types of account, and to audit compliance.

6.27. The Commissioner understands that:

6.27.1. The compromised Account had been incorrectly labelled as a 'service account'. Because there was no human user to which the Account related, there was no prompt on log-in to update the password when the new policy came into force in 2012.

6.27.2. The compromised Account should have had a manual password reset to comply with the minimum password standards enforced as part of the July 2019 update to the Active Directory, but this was not done (in part because there was insufficient monitoring of the Account) and the password on the Account remained non-compliant.

6.27.3. The Account was not identified at any time as having a non-compliant password, either as part of the 2019 IT Health check or otherwise.

6.28. In relation to this failure, it appears to be agreed that the compromised Account did not adhere to any documented password policy. The username and password of the compromised Account were both 'kiosk' – these credentials did not comply with LBoH's password policy standards.

6.29. The Commissioner takes the view that if the credentials on the Account had been compliant with a higher security standard, as set out in LBoH's password policy, it is less likely the Account would have been capable of being accessed without authorisation, or at the very least would have delayed the attempts of any potential attacker from exploiting the Account. The purpose of the policy requiring more complex passwords itself recognises that these materially reduce the risk of unauthorised access, and the fact that the Account should also have had MFA (but did not because of the engineer's error) is no answer to the point.

6.30. The Commissioner cannot conclusively conclude that a more complex password would not have been breached. However, the password was objectively weak[52], particularly in light of the data processed by LBoH's systems, and did not even adhere to LBoH's own password policy. Had LBoH adopted more robust credentials on the Account, which were compliant with an established policy, then this would have been a factor for the Commissioner to consider in determining whether appropriate steps had been taken to protect the personal data.

6.31. The Commissioner's concern also extends to the fact that there were insufficient measures in place to ensure that LBoH's password policy was adhered to across its entire network in practice. There was no process in place to ensure password-compliance for those accounts which were either dormant, did not have human users and/or were treated as 'service accounts'.

6.32. LBoH appears to have relied on log-in prompts to secure compliance with its password policy. However, this was ineffective for those accounts which were dormant, did not have human users and/or were treated as 'service accounts'. LBoH needed to have in place a process for ensuring that these accounts also complied with the minimum password policies, where necessary through manual intervention. There is no evidence of any such process being put in place in 2012 when the new policy requiring minimum password standards was adopted or, more importantly, in 2019 (post implementation of the GDPR) following the IT health check which identified issues with password non-compliance. It appears that no steps were taken to perform a manual update on those passwords which were not human accounts, but rather related to scripts or automated processes or had been labelled as such.

6.33. It does not appear that an effective audit system was put in place to check, on an ongoing basis, that all accounts with access to LBoH's system were compliant with the password policy. There does not appear to have been any audit in the period between the implementation date of the GDPR and

[52] The affected password and username were both 'kiosk'.

the July 2019 IT Health check (this in any event failed to identify the Account as being non-compliant with the password requirements) and the draft Audit Report identifies the Account on the basis that this is dormant (rather than that it failed to comply with password requirements).

6.34. The Commissioner concludes that it is not sufficient for LBoH to simply rely on the fact that it has a password policy and MFA in place as evidence that it has adhered to its duties, without also having in place appropriate organisational measures to ensure that policy and process was being applied effectively across all of LBoH's accounts.

6.35. If either the dormant Account had been identified and deactivated at some point in the eight years preceding the Attack, or the password on the Account had been in compliance with (and was ensured to be in compliance with) LBoH's password policy, it is unlikely that the Attacker would have been able to exploit the Account and gain initial access to LBoH's systems.

6.36. In making a finding that LBoH has fallen short of its duties under Articles 5(1)(f) and 32 UK GDPR, the Commissioner has considered the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Taking these points in turn:

State of the art

6.37. The management of access controls is important in protecting against unauthorised access to data processing systems. Such management includes performing on-going reviews to ensure accounts are still appropriately secured. This is in line with industry standards and guidance, for example:

- The Commissioner's Security Outcomes guidance[53] states:

  "*You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights*."

- The Cabinet Office's Minimum Cyber Security Standard[54] states:

  "*Periodic reviews should also take place to ensure appropriate access is maintained*."

(The following guidance post-dates the Attack, however it serves to demonstrate the continuing importance of appropriate user account management.)

[53] GDPR security outcomes - NCSC.GOV.UK

[54] 25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf (publishing.service.gov.uk)

- ISO27001[55] guidance states:

> "*Asset owners shall review users' access rights at regular intervals*."

Costs

6.38. In terms of the costs of implementation to remedy the established issues, there were no procurement costs involved relating to new software or hardware that were not already in place prior the Attack. The cost to LBoH would have been solely in relation to human resources expenditure in the context of drafting and implementing appropriate policies and processes, which the Commissioner's finds would have been reasonable in order to ensure that any accounts through which LBoH's systems could be compromised were being controlled.

Nature, scope, context and purposes of processing

6.39. Given the volume and nature of the data processed by LBoH, the Commissioner maintains the view that the failure to have in place measures to identify/ audit all accounts on LBoH's servers, and the failure to ensure that its password policy was enforced across its whole estate, constitutes a failure to implement appropriate technical and organisational measures in order to ensure appropriate security, in breach of Article 5(1)(f) UK GDPR.

6.40. Furthermore, it indicates a failure to ensure the ongoing confidentiality, integrity and availability of its data processing systems and services (a breach of Article 32(1)(b) UK GDPR) by reason of (i) the failure to put in place appropriate measures to identify and disable dormant accounts and regularly review and audit access controls and (ii) the failure to put in place appropriate measures to enforce the password policy in respect of all types of account and to audit compliance with its password policy.

Duration

6.41. In terms of the duration of this infringement, the issues identified above were in existence at the time of the implementation of GDPR on 25 May 2018 and were not resolved until the affected Account was taken offline on 11 October 2020.

Conclusion

6.42. The Commissioner takes the view that the security duty under Articles 5(1)(f) and 32(1)(b) UK GDPR required an organisation such as LBoH to implement appropriate measures to identify and disable dormant accounts, and to regularly review and audit access controls. For the reason explained above, the Commissioner is not satisfied that LBoH did this. Furthermore, the Commissioner finds that LBoH was obligated, but failed, to implement

[55] ISO - ISO/IEC 27001 and related standards — Information security management

appropriate measures to enforce appropriate password policies in respect of all types of account and to audit compliance.

6.43. Therefore, the Commissioner maintains the view that LBoH failed to implement appropriate technical and organisational measures in order to ensure an appropriate level of security for the personal data which it processed, and this failure constitutes an infringement of both Article 5(1)(f) and Article 32(1)(b) UK GDPR.

7. Remedial Steps Taken Following the Attack

7.1. In the time immediately following the Attack, the Commissioner acknowledges that LBoH:

- Included the details of the Attack within its Hackney Life Publication. This has been sent to 100,000 housing address throughout Hackney. An additional 8,000 copies have been put in public places around Hackney, for example, public facing council service desks.

- It updated its website informing individuals of the attack.

- It emailed all individuals who had consented to receiving marketing information from Hackney about the attack.

- It notified and engaged with the NCA, NCSC and the Metropolitan Police who created contingency plans to remove any unlawfully published data (not withstanding it was unable to exercise the plan).

- It created risk assessments to identify its high risks individuals and had plans in place should it become aware of any of the high-risk individuals' data being exfiltrated.

- It carried out 230 notifications in total, some of which were in-person, providing information about the Attack and measures to mitigate the risks.

- Data that posed a risk to life or public protection was acted upon immediately by the Metropolitan Police as per Article 2 of the Human Rights Act right to life[56], following the JESIP (joint decision model) as per its agreed data review plan, and following its agreed joint process for vulnerable adults and children.

- It created emergency intermediate business processes in response to the attack.

7.2. The Commissioner has also considered and welcomes the wider remedial steps taken by LBoH, which included isolating the affected workstation/network from the internet on 11 October 2020 following the Attack. It is understood that the network has not been reinstated and a new

[56] Principles for joint working - JESIP Website

[redacted] has been built which includes a 'zero trust' network model which is designed to provide strong mitigation against ransomware attacks. The rebuilding process included penetration testing by BAE Systems.

7.3. Furthermore, it is noted that since the time of the Attack, LBoH has implemented more regular internal vulnerability scans to bolster its internal security[57]. LBoH has also advised the Commissioner[58] that it is "[redacted]."

7.4. Since the attack, LBoH has worked on recovering its systems in relation to the resident-facing services which were most seriously impacted. Amongst those, it advised the Commissioner on 10 February 2023 that the following progress had been made:

- [redacted] – "*The system was recovered in April 2021 (by a new reinstallation of the software using recovered data). This was followed by work to reconcile data relating to the continuity arrangements, process the backlog of updates that had accumulated while the system was offline (as well as normal business as usual workloads and exceptional additional work to process Covid relief grants).* [redacted] *returned to normal service in July 2022 and* [redacted] *returned to normal service by September 2022.*"

- [redacted] – "*Due to the very large volume of* [redacted] *cases that Hackney manages, work to restore normal service was completed in December 2022.*"

- [redacted] – "*The attack meant that the* [redacted] *system was unavailable but the* [redacted] *system was unaffected as this is externally provided. Work to deliver new* [redacted] *software completed in September 2022 and work is now well advanced to update the Council's* [redacted] *with new applications and details of changes of circumstances.*"

- [redacted] – "[redacted] *were impacted by the attack and the Council was initially unable to process these. […]. Early in 2021 a* [redacted] *service was made available using recovered data and the* [redacted] *team were able to process* [redacted] *requests using this service. Work to clear backlogs of work and return to normal workloads was completed in spring 2022. Work continues to recover all data required to provide a full*[redacted] *service […].*"

[57] In its Initial Representations (§24(6)) LBoH indicated that it "*has since introduced monthly internal scanning",* however it has since suggested that its internal vulnerability scanning may now be even more regular than this.
[58] Letter from LBoH to the Commissioner, 10 February 2023

- [redacted] – "*The Council's [redacted] system [redacted] was impacted by the attack and rendered unavailable. Immediately after the attack, work was prioritised to provide interim case recording tools for [redacted] so that structured case records could be maintained. Work also took place to review available data to help identify people who might be at risk and prioritise [redacted] activities. […]. Work took place to use recovered data to rebuild a clean (hosted) installation of the [redacted] system. This went live as a read-only reference in June 2021, as a full system for [redacted] in April 2022 and for [redacted] in December 2022. […]. Recognising that there would be an extended timeframe for recovering the [redacted] system, a parallel work programme took place to develop open source software that would provide access to recovered data and enable case recording. This went live as a read-only reference in March 2021 and was updated to record new case information from June 2021.*"

- [redacted] – "*At the time of the cyberattack the Council was working to decommission its [redacted], including planning migration of files to the [redacted] service. The attack resulted in [redacted] being unavailable and the Council has only been able to carry out a partial recovery of data that was held in the [redacted] system. In some cases the Council has been able to recover files and sufficient metadata to migrate service files to [redacted] (or other systems if appropriate). In other cases this has not been possible and the Council's team is working to provide a search service that will enable services with essential business need to request files that were held in [redacted] and for the ICT team to identify whether files can be made available.*"

7.5. LBoH further advised that since the Attack it now uses "[redacted]."

8. The Commissioner's Discretion to issue a Reprimand

8.1. In reaching a decision on this matter as to whether it is appropriate and proportionate to take enforcement action, the Commissioner has given due consideration to the non-exhaustive criteria set out within the Regulatory Action Policy[59]. This Policy is referred to within the NOI and the December Letter[60] and the criteria includes consideration of:

[59] Regulatory Action Policy (ico.org.uk)

[60] NOI, §4.1; and the December Letter, §2.62.

- *the nature and seriousness of the breach or potential breach (including, for example, whether any critical national infrastructure or service is involved);*

- *where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion;*

- *the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy;*

- *whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data;*

- *the gravity and duration of a breach or potential breach;*

- *whether the organisation or individual involved is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if not addressed;*

- *the cost of measures to mitigate any risk, issue or harm;*

- *the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute);*

- *whether another regulator, law enforcement bodies or competent authority is already taking (or has already taken) action in respect of the same matter; and,*

- *in relevant cases, the expressed opinions of the European Data Protection Board.*

8.2. In considering these factors, the Commissioner considers that the following matters are relevant.

8.3. The range of systems within which data was encrypted by the Attack are listed at §3.4 of this Reprimand. The Commissioner understands that the data held by LBoH within these affected systems included data revealing racial or ethnic origin, religious beliefs, sexual orientation, health data, economic data, criminal offence data, and other data including basic personal identifiers. As evidenced by the nature of the systems which were affected, some of the individuals whose data was compromised were among the most vulnerable in society, and they had trusted LBoH to safeguard their personal data.

8.4. The Commissioner takes note that – by LBoH's calculations – of the 440,000 records affected by the encryption (of which personal data relating to not less than 280,000 individuals was affected), a total of 9,605 records are

understood to have been exfiltrated[61]. A quantity of this data was understood to have been published on the dark web[62]. The Commissioner also has taken into account of the nature of the data exfiltrated, which was subsequently published on the dark web, which is understood to have included [redacted][63], [redacted][64], [redacted][65].

8.5. The Commissioner takes the view that the types of personal data being processed by LBoH – which related to no less than 280,000 individuals - were the type which were of high risk and that could cause, or be likely to cause, a real and significant risk of damage.

8.6. The Commissioner considers that the personal data that LBoH was processing was high risk for the following reasons:

- It related to a large number of individuals and contained a large amount of personal data;
- It was processing the types of personal data that can potentially be used in identity fraud (for example, [redacted]);
- It was processing the types of personal data that can potentially give rise to damage of a person's reputation. For example, [redacted];
- It was processing personal data relating to a person's health, for example, [redacted];
- It was processing personal data relating to vulnerable individuals, for example, [redacted];

[61] Initial Representations, §35(2), Further Representations, §34(2)(i).

[62] As per §3.15 above, on 6 January 2021, LBoH was notified by the NCA that a collection of the exfiltrated data had been published.

[63] [redacted].

[64] As per the information provided in Appendix B of LBoH's letter to the Commissioner, 28 May 2021, this exfiltrated data included: references to [redacted]

[65] Which included [redacted].

- It was processing personal data that could put individuals at significant risk of harm, for example, [redacted];

- It was processing personal data that individuals would typically expect to remain confidential between the data subject and LBoH, for example, [redacted].

8.7. This personal data required robust and strong levels of security, and it is reasonable to expect this security to be in line with industry standards. LBoH fell short in this regard and in doing so, the privacy rights of not less than 280,000 individuals were impacted by the encryption, not least by the loss of confidentiality of their personal data, some of which included their special category data, and/or was particularly sensitive.

8.8. Furthermore, in terms of the encryption of data on the affected systems, the resulting loss of access is also understood to have impacted LBoH's services, not least in relation to its ability to deal with FOI (Freedom of Information) requests and the rights of data subjects via subject access requests (SARs). For instance, the Commissioner received 39 complaints from individuals between August and October 2020, during which time 70 SARs were made to LBoH.

8.9. In relation to some of the SARs, the Commissioner received a number of complaints from individuals to say that they had encountered problems in accessing their data from LBoH following the Attack, with some complaints expressing concern that their data would be irrecoverable[66]. Some such examples include:

- (Dated 15 October 2021) An individual who had been born into care and was trying to establish information about their past. LBoH had advised that individual that it did not know if or when systems would be accessible and that they felt like their "*whole history has been wiped and I will not be able to find the answers I'm looking for, to simple things like names of grand parents*".

- (Dated 13 July 2021) An individual who had been adopted at birth and over the last year had started to take action to find out more information about their adoption, stating that he was "*fearful that [LBoH] may not be able to reinstate my files at all – and, 8 months on, they show no signs of being able to*".

[66] The Commissioner makes no finding as to the allegations expressed in some of the complaints that data may be irrecoverable as a result of the Attack. LBoH has explained that it "*has successfully recovered the data needed to rebuild its service systems and is generally able to search for and recover data in individual cases*" (LBoH's Submissions of 14 May 2024, §3(3)(III))

- (Dated 7 July 2021) An individual complained that his "*personal data had been affected by the recent cyber attack that led to personal information being leaked. This has caused me great concern both mentally and physically. The media stories have only added to my distress*".

8.10. In addition to a disruption in LBoH's responses to FOI requests and SARs, it also impacted their ability to operate as a council. Without access to their processing systems and the data contained within, LBoH could not effectively operate as required, and provide certain services to their constituents.

8.11. This was demonstrated by a publication on LBoH's website some months after the Attack[67] which cited a significant ongoing disruption to a number of its services, including: [redacted].

8.12. Regarding the exfiltrated data, LBoH accepts that there was a "*meaningful risk of harm*" to 230 individuals[68]. It is understood that some of the exfiltrated data related to children, although there is no breakdown for the number of affected children. However, any exfiltrated personal data relating to children would have been particular sensitive. For example, some of the exfiltrated records included [redacted].
The Commissioner is mindful of Recital 38 UK GDPR in this regard, and of the UN Convention on the Rights of a Child[69] which also merit children with the right of respect to their privacy, family and home life. [redacted].

8.13. In the Commissioner's view, the fact that only a portion of the encrypted data was confirmed to have been exfiltrated is not wholly determinative of the seriousness of this infringement. This is because the legislation expects confidentiality of all data held to be protected. In this instance, loss of confidentiality affected not less than 280,000 individuals. The Attacker had access to all of this information, and there is no way of knowing conclusively what happened to that data once the Attacker had access[70]. It is the Commissioner's position that publishing information would not have been the only means of exploiting this data, and the Commissioner would point

[67] As of 15 March 2021
[68] Initial Representations, §35(3).
[69] UN Convention on the Rights of a Child (unicef.org.uk)
[70] It should be noted that the Commissioner does not make a finding that all of the data which was encrypted was 'positively accessed' by the Attacker. However, the Commissioner is satisfied that the Attacker had the ability to positively access that data if they so wished, by virtue of the control they had gained in carrying out the Attack. This Attack resulted in the loss of access to, and availability of, the personal data held on LBoH's systems.

to the examples provided at §8.9 above as evidence of the demonstrable harm which exists outside of mere exfiltration.

8.14. Regarding the duration of the failures which are causally relevant to the Attack:

8.14.1. In terms of the patch management issues, the Commissioner repeats the comments at §5.39 above, noting that the necessary patch to counter the CVE-2020-0787 vulnerability was released on 10 March 2020, but was not appropriately applied to the relevant workstation so as to prevent the attacker from being able to exploit the vulnerability to gain privileged access. This vulnerability was not fixed until post-incident, on 11 October 2020.

8.14.2. Regarding the account management issues, the Commissioner repeats the comments at §6.41 above, and takes a view that LBoH's failure to ensure appropriate processes in place to identify and decommission the dormant Account and to ensure that the passwords used across all of the devices on its network were compliant with its policy existed since at least 25 May 2018 (i.e. the implementation date for the GDPR) and continued through to the Attack in October 2020. Had the User Account Management issues identified above been addressed promptly, or identified at any point prior to the audit in April 2020 and resolved as they reasonably ought to have been, this would have likely resolved the issue for the Account (which had lain dormant since 2012), prior to any attack taking place.

8.15. The Commissioner has considered the costs of implementing the measures which would have prevented this incident[71], which appear to be relatively minimal. In terms of the human cost of implementing these measures, whilst the Commissioner is sensitive to the significant burden imposed by the COVID-19 pandemic, for the reasons outlined at §§6.22 – 6.24, and later at §§8.32 – 8.33, he takes the view that if LBoH had had proper processes in place as required, then the impact of the pandemic would have been less of a factor as the issues would have been adequately addressed prior to Spring 2020. He has also considered LBoH's claim at §46 of its Initial Representations that the financial impact of the Attack on LBoH is "*over £12.5M*".

8.16. Furthermore, the Commissioner has considered the public interest in regulatory action being taken, noting in particular the deterrent effect which it would have on both LBoH (not least in engaging senior leaders to ensure appropriate oversight of the measures it invests in) but also, importantly, on other Controllers and Processors to ensure they understand and uphold their duty to protect the personal data of the UK public.

[71] Above at §§5.35 – 5.37 (patch management); and §6.38 (account management).

8.17. LBoH has alleged in its Representations that the Commissioner has overstated a number of matters in its findings and has understated others[72]. Accordingly, it says that the Commissioner cannot fairly or otherwise lawfully conclude that this is a case where a Reprimand is warranted or otherwise appropriate.

8.18. The Representations on this point may be broadly summarised as follows:

8.19. The Commissioner has overstated the following issues:

- Seriousness;
- Risk of harm; and,
- Causal relevance.

8.20. Furthermore, the Commissioner has understated the following issues:

- LBoH's wider commitment to data security;
- The impact of the COVID-19 pandemic; and,
- The risk of prospective third-party claims against LBoH, and the reputational impact of a Reprimand.

8.21. In relation to these issues, the Commissioner's conclusions are as follows:

Seriousness

8.22. The types of personal data being processed by LBoH were the type that could cause real and significant risk of damage, in particular taking into account that the affected individuals were some of the most vulnerable in society. The types of data affected by this attack are outlined above at §§3.5; and 8.3 of this Reprimand, and the Commissioner would maintain that the loss of confidentiality and availability of such data could, and did by LBoH's own case, lead to a risk of harm to individuals, not least noting that the encrypted data included data which could be classified as special category data, or highly sensitive.

8.23. Further, the Commissioner takes the view in this case that this Attack had serious (or potentially serious) implications for not less than 280,000 affected data subjects. LBoH is a public authority with responsibility for processing large volumes of personal data (including special category data), and the failings identified by the Commissioner in the course of his NOI, December Letter, and this Reprimand are not matters which required significant resources to correct.

Risk of harm

8.24. In terms of the risk of harm to affected data subjects, the Commissioner's position is that the impact of the encryption of data led to a significant loss of confidentiality and availability of data for not less than 280,000

[72]Initial Representations, §§10 – 12, 29 - 50; and Further Representations, §§3(5); 33 – 36.

individuals, with personal data and special category data being accessible by malicious actors, and subject to significant risk of exfiltration[73].

8.25. It is understood that, as of 30 June 2021, LBoH had received approximately 140 enquiries into its dedicated inbox which was created in response to this Attack. It stated that the vast majority of the enquiries were general enquiries regarding personal data and the wider extent of the Attack. However, LBoH considered that 10 of these could be considered as informal complaints. LBoH indicated that some individuals had indicated a degree of anxiety, stress, worry or fear. In response, LBoH provided support to help mitigate this, including a dedicated personal direct line to a Senior Council Officer and provision of ID Theft and Anti-Fraud protection where appropriate[74].

8.26. In addition to the above, as explained at §§8.8 – 8.11, this encryption had a significant impact on LBoH's services and its abilities to conduct its business as a council.

8.27. Furthermore, there was a significant risk of harm from the exfiltration of data in terms of the information which was compromised through publication on the dark web. The data impacted by this exfiltration is known to have consisted of the data referred to at §8.4 above. This, on LBoH's own case, involved a meaningful risk of harm to 230 data subjects[75].

Causal relevance

8.28. The Commissioner finds that the failures identified in relation to the patch management and user account management did directly contribute to the Attack for the reasons outlined in the NOI, the December Letter, and this Reprimand. Had the relevant patch been appropriately applied, the attacker would likely have been unable to exploit the vulnerability to gain privileged access, and had either the dormant Account been identified and deactivated prior to the Attack, or the password on the Account been in compliance with (and was ensured to be in compliance with) LBoH's password policy, it is unlikely that the Attacker would have been able to exploit the vulnerable Account.

8.29. The Commissioner notes that this Representation regarding causal relevance appears to have been more specifically directed at the Commissioner's preliminary findings in relation to LBoH's internal vulnerability scanning and firewall procedures. As explained at §1.6 of this Reprimand, these preliminary findings are not being maintained for the purposes of this Reprimand.

---

[73] In terms of the assessment of damage suffered by affected data subjects, the Commissioner has regard to Recital 85 UK GDPR which explains that "*physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*".

[74] LBoH's response to ICO enquiries of 9 June 2021.

[75] Initial Representations, §35(3).

Wider commitment to data security

8.30. The Commissioner is satisfied that, aside from in the circumstances which gave rise to this Attack, LBoH has otherwise demonstrated satisfactory data protection compliance. In particular the Commissioner is mindful of, and commends, LBoH's good governance structures, policies, improvement plans and training and development of staff.

8.31. The Commissioner further acknowledges the significant remedial steps taken by LBoH in response to this Attack as outlined at §7 of this Reprimand. Such steps have included transparency with the public and the data subjects affected; open engagement with the appropriate enforcement agencies; and the adoption of a [redacted], designed to provide protection against future ransomware attacks.

8.32. However, whilst the Commissioner acknowledges LBoH's generally good compliance, and recognises the measures that it has taken since the Attack to further improve its compliance with data protection legislation[76], the Commissioner notes that the infringements in relation to appropriate policies and procedures which are relevant to the patch management and user account management issues pre-date the COVID-19 pandemic; with the infringements resulting in deficiencies which would not indicate an organisation that was operating at an adequate level of data security in these particular respects.

Impact of COVID-19

8.33. The Commissioner has considered and acknowledged the impact of the COVID-19 pandemic and its impact on the resources of organisations like LBoH. The Commissioner is sympathetic and has taken account of the considerable demands on the LBoH at an organisation-wide level, together with the stresses and demands on particular individuals with responsibility for matters relating to data security. However those demands, and the difficulties experienced by many public authorities during the course of the pandemic, cannot be unquestionably relied upon to excuse organisations from their obligations to ensure appropriate data security, particularly in circumstances where failings existed before the pandemic. Further, whilst the Commissioner understands that resources may have been Limited at the time of the Attack, the particular failings identified are not matters which required extensive resources to address either in terms of finance or time.

Risk of third-party claims and reputational impact

8.34. The Commissioner respectfully notes that the risk of third-party claims against LBoH exists irrespective of any potential enforcement action that the Commissioner may take, not least because the Attack has already been publicised widely in the public domain. The possibility of potential claims

[76] Further information provided at §7.

against LBoH is not a matter upon which the Commission would place – or be required to place - material weight in determining whether it is appropriate and proportionate to take enforcement action in a given case.

8.35. Similarly, LBoH cite the potential reputational harm of receiving a Reprimand, however this is not something in this case which the Commissioner gives considerable weight to, given that the investigation has found that LBoH is responsible for a serious data breach. It follows that there should be public accountability for such a failure.

8.36. In any event, the Commissioner has noted the steps taken since by LBoH to improve data protection compliance. This arguably mitigates any risk of negative reputational impact given these detailed remedial steps are set out in this Reprimand.

8.37. Having considered all of the above, the Commissioner's position is that the proposed regulatory action would be effective, proportionate and dissuasive.

8.38. Article 58 UK GDPR, and the Commissioner's Regulatory Action Policy[77], set out a range of powers available to the Commissioner. The Further Representations suggest that the Commissioner appears to have failed to consider other routes to helping LBoH to improve its compliance, and provides the examples of an audit or informal undertakings, which it suggests may be more appropriate[78]. The Commissioner would highlight that audits are an investigative power[79] which may be utilised to enable the Commissioner to better understand an issue or to assess current compliance, and accordingly would not be necessary or appropriate in this instance. In terms of an informal undertaking, this too would not be appropriate in circumstances where there have been serious infringements of the UK GDPR, given that it holds no legal standing.

8.39. The Commissioner had initially been minded to impose a monetary penalty in this case. However, in light of the Commissioner's public sector approach[80], and having considered the wider factors in this case, the Commissioner takes the view that a Reprimand is an appropriate and proportionate use of his regulatory powers in this instance.

9. Conclusion

9.1. For the reasons outlined above, the Commissioner takes the view that LBoH has contravened Articles 5(1)(f) and 32(1)(b) of UK GDPR. As detailed within the Commissioner's Regulatory Action Policy[81], the Commissioner has a range of regulatory tools at his disposal including the imposition of

[77] Regulatory Action Policy (ico.org.uk)
[78] Further Representations, §2(4)(i).
[79] Article 58(1)(b) UK GDPR.
[80] ICO sets out revised approach to public sector enforcement | ICO
[81] Regulatory Action Policy (ico.org.uk)

administrative penalties, enforcement notices, and Reprimands which can be used where it is appropriate to do so.

9.2. Having examined the circumstances of this case, the Commissioner had initially considered that an administrative penalty in the sum of £1,350,000 would be appropriate, and considered notifying LBoH of its intention to impose such an administrative penalty[82]. However, since June 2022 the Commissioner has adopted a revised approach to public sector enforcement and, on this occasion, the Commissioner has decided not to impose an administrative penalty[83].

9.3. Taking into account all the circumstances of this case, including the Representations made by LBoH, the remedial steps detailed above and LBoH's broader commitment and adherence to data protection compliance, the Commissioner has decided that it would be appropriate to issue a reprimand to LBoH in relation to the infringements of Articles of the UK GDPR set out above. Furthermore, the Commissioner considers that this course of action is appropriate, proportionate, and in the public interest.

Dated: The 5th day of July 2024

Stephen Bonner, Deputy Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

[82] The initial proposed penalty amount of £1,350,000 was predicated on a preliminary finding – as outlined in the NOI - that LBoH had infringed the UK GDPR in four respects under Articles 5(1)(f) and 32(1), i.e. inadequate patch management, insufficient user account management, insufficient internal vulnerability scanning, and inadequate firewall policies /procedures. Following consideration of LBoH's Representations, and for the reasons outlined in this Reprimand, only two of these preliminary findings are maintained for the purpose of this enforcement action.

[83] ICO sets out revised approach to public sector enforcement | ICO.