The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

To: Levales Solicitors LLP

Of: Unit 1, 378-380 Vale Road, Ash Vale, Aldershot, Hampshire, GU12 5NJ

The Information Commissioner (the Commissioner) issues a reprimand to Levales Solicitors LLP in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (GDPR) in respect of certain infringements of the UK GDPR.

1. **Summary of Incident**

1.1. Levales Solicitors LLP is a law firm, founded in 2010, specialising in criminal and military law.

1.2. The breach occurred after an unknown threat actor gained access to the secure cloud based server via legitimate credentials, later publishing the data on the dark web.

1.3. In total, 8,234 UK data subjects were affected, of which 863 were deemed to be at 'high-risk' of harm or detriment due to the special category of data including criminal data pertaining to 'homicide, terrorism, sexual offences, offences involving children or particularly vulnerable adults'. The full list of affected data involved includes:

- Name
- Data of Birth
- Address
- National Insurance Number
- Prisoner Number
- Health Status
- Details of Criminal allegations not charged
- Details of Criminal allegations prosecuted
- Outcomes of investigations and prosecutions
- Details of complainants and victims both adult and children
- Previous Convictions
- Legally privileged information and advice

2. The reprimand

2.1. The Commissioner has decided to issue a reprimand to Levales Solicitors LLP in respect of the following infringements of the UK GDPR:

- Article 32(1)(b) which states organisations should be able to "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

- Article 32(1)(d) which states "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"

2.2. Our investigation found infringements in relation to the security requirements of the UK GDPR. The reasons for the Commissioner's findings are set out below.

3. Article 32(1)(b)

- Levales Solicitors LLP were not ensuring the ongoing confidentiality of it's processing systems as per Article 32(1)(b).

3.1. Levales Solicitors LLP did not have Multi-Factor Authentication (MFA) in place for the affected domain account. Levales relied on computer prompts for the management and strength of password and did not have a password policy in place at the time of the incident. The threat actor was able to gain access to the administrator level account via compromised account credentials. Levales Solicitors LLP have not been able to confirm how these were obtained.

3.2. MFA is a basic measure we would expect to see organisations processing personal data implement, regardless of risk of

processing. Guidance was available on both the ICO[1] and NCSC[2]'s websites highlighting the importance of using MFA when storing sensitive data or data that could cause significant harm if compromised.

4. **Article 32(1)(d)**

- Levales Solicitors LLP did not implement appropriate organisational measures as per Article 32(1)(d).

4.1. Levales Solicitors LLP did not implement appropriate technical and organisational measures to ensure their systems were secure. Levales outsourced their IT management to a third party and were unaware of security measures in place at the time of the incident, such as detection, prevention, and monitoring. Levales had not reviewed if the technical measures associated with the contract, were appropriate for the personal data they were processing since the contract was first signed in 2012.

4.2. When using a managed service provider, the ICO would expect that contracts are reviewed and that the responsibilities within the contract are fully understood to ensure the security of the data being processed is upheld. The NCSC[3] provides a 12 step guide, which highlights that any vulnerabilities within the contract between provider and controller, with regards to security, can be exploited easily by threat actors.

5. **Remedial steps taken by Levales Solicitors LLP**

5.1. The Commissioner has also considered and welcomes the remedial steps taken by Levales Solicitors LLP in the light of this incident. In particular the introduction of MFA for all user accounts, updated service contracts with third party providers, and a complete review of their existing systems to prioritise work and upgrades to the firewall.

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/passwords-in-online-services/
[2] https://www.ncsc.gov.uk/collection/zero-trust-architecture/authenticate-and-authorise
[3] https://www.ncsc.gov.uk/collection/supply-chain-security

The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

6. Decision to issue a reprimand

6.1. Taking into account all of the circumstances of this case, including the remedial steps taken, the Commissioner has decided to issue a reprimand to Levales Solicitors LLP in relation to the infringements of Article 32(1)(b) and Article 32(1)(d) of the UK GDPR set out above.[4]

[4] Levales Solicitors LLP has had an opportunity to make representations to the Commissioner in response to the Notice of Intent regarding this reprimand. Levales Solicitors LLP did not provide a response.