THE LABOUR PARTY LEAKS: DATA PROTECTION RISKS FOR POLITICAL PARTIES AND CAMPAIGNERS

Date: 20 April 2020

UK Electoral Law Group and Data Protection, Privacy, and Security Alert

By: Dylan G. Moses, Rosie Naylor, Piers Coleman, Alexander J. Bradley-Sitch

BACKGROUND

Over the Easter weekend, it was reported by a number of media outlets that an 860-page report, apparently commissioned by senior Labour Party officials, had been leaked and was circulating widely online. The leaked report purports to show that factional hostility against Jeremy Corbyn prevented senior Labour Party officials from effectively dealing with alleged antisemitism within the party.

Having being shared with news outlets, including reportedly Sky News and the Guardian, the report began to be shared on social media. Notably, it was reported on social media that the report may have been shared on Facebook by a member of the Shadow Cabinet in a now-deleted post. The political consequences of this document and its origins are likely to be argued over for some time to come, particularly against the background of Sir Keir Starmer's recent election as Leader of the Labour Party.

But what of the legal consequences? It has been reported that the report contains unredacted personal data of numerous current and former Labour party staffers who raised complaints about alleged antisemitism during Jeremy Corbyn's tenure as Leader. The Information Commissioner's Office (the “ICO”) is the government body responsible for enforcing data protection laws in the UK. It has the power to investigate and issue fines against anyone in breach of data protection principles.

This story is a timely reminder that all political parties and campaigns should be aware of their obligations, and the potential risks, when it comes to collecting and storing personal data.

WHAT OBLIGATIONS MUST POLITICAL GROUPS AND CAMPAIGNS COMPLY WITH?

The General Data Protection Regulation (“GDPR”) greatly expanded the obligations on “controllers”[1] and “processors”[2] of personal data. In many instances, political parties are likely to be deemed controllers. They will maintain personal data about their employees, registered members, and individuals who are signed up to receive emails and newsletters.[3]

Processors could include any entity with which the political party or campaign group shares information, such as campaigning groups, individual MPs or employees, and firms engaged to provide strategic or PR advice.

Controllers of personal data have numerous duties in respect of the personal data they control or process. For example, controllers are required to have proper security measures in place to protect personal data; they must carry out a data privacy impact assessment prior to controlling or processing data; and they must maintain proper records. They must notify data subjects if there has been a breach or a leak and data subjects must be able to raise subject access requests with controllers to access personal information held by controllers. Processors have similar duties to controllers, albeit they are somewhat less onerous.

There are exemptions in the GDPR and under the Data Protection Act 2018 (the “DPA 2018”) which can be relied upon by a controller or processor to prevent them for being subject to sanctions in certain cases. However, the ICO advises against relying on exemptions in a blanket fashion and they should be carefully considered on a case-by-case basis. Organisations should justify and document their reasons for relying on an exemption so that they can demonstrate compliance.

WHAT RISKS DO POLITICAL PARTIES AND CAMPAIGNERS FACE?

All membership organisations face legal and compliance risks related to the collection and retention of personal data. Political parties, with particularly large membership bases, face these risks more than most.

Further, they are likely to hold more extensive data about their members, including information about religious and political beliefs, economic background, and other acutely sensitive data. On top of this, often parties will not have the same resources or internal know-how as the commercial sector. As a result, a failure to comply with regulations relating to the collection and retention of personal data can lead to serious penalties.

In the event that personal data is compromised, as the result of a data loss or leak, the consequences will be even more serious. In addition to financial costs and liabilities, organisations almost inevitably suffer reputational damage which it is necessary to mitigate following a major data loss, and for political campaigns, serious reputational damage can be an existential risk.

INVESTIGATIONS

In the immediate wake of a data loss scenario, it is likely that advisers such as cyber security professionals and lawyers will need to be retained to conduct an independent investigation. These professionals may be able to determine the scale of the breach, identify any affected data subjects, and identify the cause of the breach.

Once the scale of the breach is understood, the data controller or processor may need to comply with its obligation to notify data subjects about the fact that their personal data has been compromised. Depending on the number of data subjects affected, this could be a major undertaking.

Regardless of the steps taken internally to identify and resolve any consequences resulting from a data loss scenario, organisations are likely to need to promptly notify the ICO of the data loss.

FINES AND DAMAGES

The ICO has the power to levy fines under the GDPR of as much as €20m or 4 per cent of an organisation's global turnover.

In addition to regulatory fines, organisations may face civil claims by anyone adversely affected by the data breach, including damages for 'distress' compensation, even if victims did not suffer financial loss as a result of the breach, and the organisation may face paying a portion of the claimants' legal costs.

CRIMINAL LIABILITIES

Entities and individuals may face criminal liabilities under GDPR and the DPA 2018. For example, section 170 of the DPA 2018 makes it a criminal offence “knowingly or recklessly… to obtain or disclose personal data without the consent of the controller”, breach of which may lead to prosecution and a fine.

The significant civil and criminal liabilities that may arise as a result of a data loss scenario highlight the importance of ensuring that adequate data protection measures are in place and that any breaches are appropriately investigated and addressed to prevent reoccurrences.

WHAT CAN POLITICAL PARTIES AND CAMPAIGNING ORGANISATIONS DO TO MITIGATE DATA PROTECTION RISK?

In the age of modern campaigning, all political organisations will collect personal data in some form. It may hold information about its members, target voters, its donors or its employees. As such, it is neither practical nor realistic to mitigate risk by simply not being a data controller or processor.

It is particularly important for political parties and campaigning organisations to ensure that they have sound risk management protocols in place. There is no universal approach to good data protection and practices should be tailored to meet your party or campaign's size, activities, and risk profile. With appropriate protocols implemented, the risk of a breach occurring can be significantly reduced.

Nevertheless, organisations should always be prepared in the event that a data loss or leak does occur, at the very least by having an effective crisis response protocol in place. Personnel should have relevant and up-to-date training on how to respond to data loss scenarios.

Like commercial organisations, political parties and campaigning organisations can purchase insurance to cover losses flowing from a data breach, either as a stand alone Cyber Policy, or as part of their wider insurance package (for example as an extension to Property Damage policies). The terms of cyber insurance can vary significantly and care should be taken to ensure the policy is appropriate for your party or campaign's risk profile.

FOOTNOTES

[1] “Controller” means any person or organisation which controls personal data

[2] “Processor” means any person or organisation who does something with personal data on behalf of a controller.

[3] “Personal data” includes any information that can be used to identify a person, including their name, locations or email addresses.

KEY CONTACTS

DYLAN G. MOSES
PARTNER

LONDON
+44.20.7360.8154
DYLAN.MOSES@KLGATES.COM

ROSIE NAYLOR
SENIOR ASSOCIATE

LONDON
+44.20.7360.8241
ROSIE.NAYLOR@KLGATES.COM