Data protection requirements for political parties 3/35/22

When it comes to personal data processing, political parties are no exception, being subject to the same requirements of the General Data Protection Regulation (GDPR) that apply to any other data controller. It's noteworthy the National Data Office has recently issued new guidelines on personal data processing in the run-up to the general election. Could this mean the regulator will be scrutinising the political parties for GDPR compliance? This article explores what measures a political party should take to ensure its data processing complies with GDPR.

Browsing the party websites leads to the conclusion that almost every one of them is incomplete and non-compliant (they lack information on securing the data subject's rights prescribed by GDPR, cookies are processed without a lawful basis etc). Since many political parties recruit their candidates and members from the business community, we will outline a number of key aspects the parties need to consider when processing personal data in the run-up to the general election.

An appropriate privacy notice

The privacy notice posted on a party's website has to state the rights of a data subject pursuant to GDPR articles 13 and 14, and the party must be able to carry those out should the data subject ask for it. Posting a privacy notice doesn't necessarily mean it complies with GDPR, so the party needs to ensure its notice is transparent, easy to understand, and designed for a particular audience, and it clearly describes the goals of data processing.

A lawful basis for data processing

Each data processing goal needs a lawful basis that has to be stated in the privacy notice. Merely claiming the party's personal data processing is legitimate doesn't necessarily mean it has a lawful basis. The party has to carefully determine a lawful basis and explain it in detail in the privacy notice (e.g. contacting an identifiable voter, providing the Anti-Corruption Office with information on payment of membership dues, processing cookies on the party's website, or storing personal data in the cloud). Each activity should be given the most appropriate lawful basis for data processing.

Appropriate consent of the data subject

The data subject's consent must be free, specific and explicit, and it must not be included in the text of forms. It's also wrong to include consent ticks in pre-marked boxes – it must be up to the data subject to put a consent tick for a particular data processing activity. In no event may the party put a voter under pressure to share their data, for instance by phoning or writing to an identifiable person on social networks and asking them to submit their data (email, address or phone number) in order to send them commercial messages. This means the data subject cannot be contacted unless the party has received explicit consent from them stating they want to be contacted about a particular offer.

Profiling, political advertising and campaigning

Political parties will often obtain personal data from third parties, such as intermediaries, in order to send notifications to a particular audience for achieving their election or campaign goals. Political affiliation may be inferred by analysing personal data from various sources (even unrelated to politics) and by evaluating the person's behaviour or making some other observations (e.g. pictures, comments and social posts). The party is liable to inform the data subject about such use of intermediary data by disclosing this in its privacy notice under GDPR article 14. It's also important for the party to run a check before using such intermediary data to see if it has been obtained lawfully.

If the party does profiling, the data subject must be informed of this data processing activity in the privacy notice and the party must be able to comply with the data subject's request should they wish to refuse profiling.

Appropriate technical solutions and organisational measures

While GDPR permits the data controller to determine what measures or solutions he will adopt to ensure his data processing complies with GDPR, this permission does not make his work much easier because he still has to assess whether any data processing done by the party is secure and compliant and whether the measures taken are adequate. The party should also be able to demonstrate it has put appropriate technical solutions in place, drawn up suitable documentation, and trained its members.

Before acquiring any external service, the party should be able to determine whether that service requires a data processing agreement. When data is transferred outside the EU/EEA, the party has to consider what guarantees it will put in place to ensure GDPR compliance.

The parties are also liable to observe the principle of accountability, which boils down to two core obligations: the duty to ensure GDPR compliance and the ability to demonstrate it. This means the controller is liable to document in writing all the rules and decisions relating to data protection.

Unfortunately, there is no single list of data protection documents to be drawn up in order to demonstrate GDPR compliance. So the parties need to assess whether they have sufficient knowledge of data protection, whether they are doing any processing activities governed by GDPR article 37, which requires them to appoint a data protection specialist or register their processing activities, and whether they are liable to draw up specific data protection documents prescribed by GDPR.

So, if your party has any doubts or questions about personal data processing, we encourage you to consult data protection specialists.