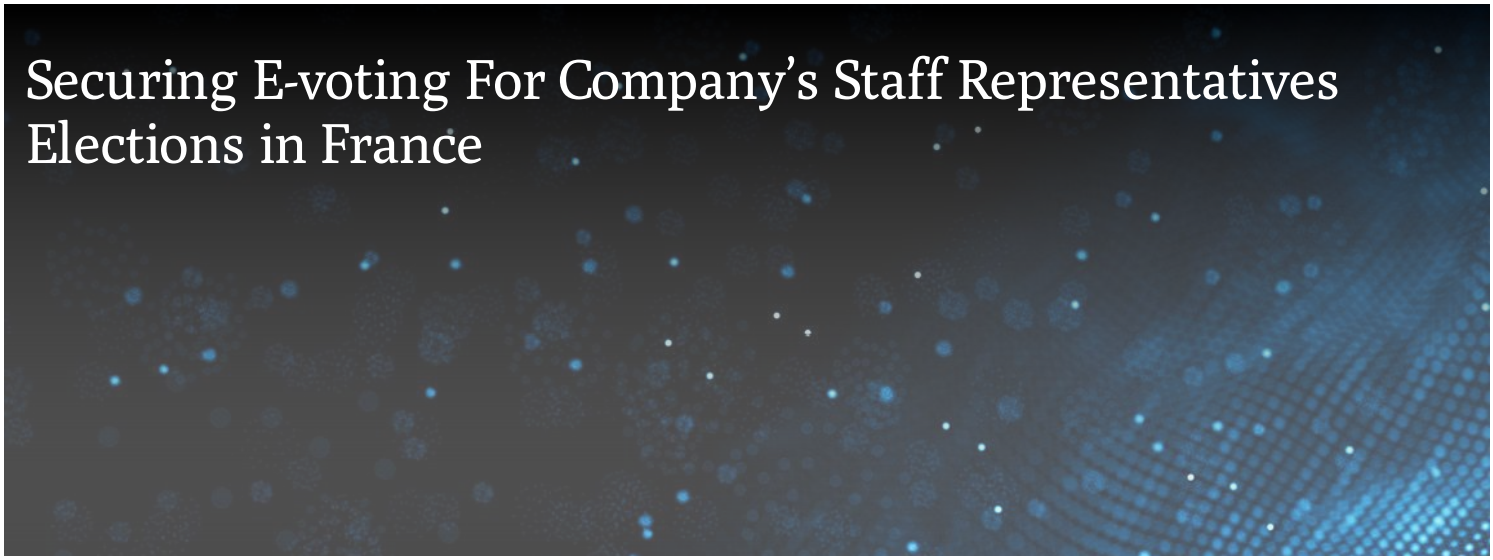
WINSTON & STRAWN LLP

BLOG

Securing E-voting For Company's Staff Representatives Elections in France



JUNE 17, 2013

There has been a significant growth in e-democracy in the last years, for all types of elections, and in many countries. E-voting improves the accessibility to the election for remote or disabled voters and allows easier and quicker counting of ballots. However, e-voting can facilitate electoral fraud or data protection breaches. The process has thus come under scrutiny by the French data protection authorities (the CNIL), to ensure that the system used for e-voting guarantees the positive identification of the voter, the anonymity and the secrecy of the vote, and the control of the electoral operations. Procedures to accomplish these measures include strong encryption measures and securization of authentication of voters (electronic certificate, computer system for processing the election located in a secure place, etc.). In a case on this topic, on May 16, 2013, further to a Trade Union's complaint, the CNIL issued a warning against Total Raffinage Marketing. Total Raffinage used the election software program "Election Central," produced by the company Election-Europe, during its September 2012 workplace elections. According to the allegations, multiple security failures were observed, constituting a violation of Article 34 of the French Data Protection Act of 1978. In particular, the data controller did not take all precautions to protect personal data: the vote was conducted without first commissioning an independent evaluation of the voting system, the company was unable to guarantee the system's correct functioning or to verify the voting results, the login user names and passwords were sent by unsecured postal mail or email, and the votes sent to the central ballot were not encrypted. A similar decision was rendered by the French Supreme Court on February 27, 2013 against Peugeot Citroën.

Tip: While electronic voting, including for workplace elections, may be possible in France, companies should take care to heed CNIL recommendations, including appointing an independent expert to ensure that the system works well, and that (1) the voter's vote (i) is not changed by the system, (ii) is taken into account, and (iii) is anonymous; (2) the ballot box is sealed and the ballots are not accessible during the election; (3) the ballots are continuously encrypted from the vote to the counting phase; and (4) the system prevents the addition of illegitimate votes.

2 Min Read

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.