SARs: a tool for identity theft

A researcher from Oxford University has sent a fake subject access request to over 150 companies in order to prove how the “right of access” under Article 15 of the GDPR can be easily exploited by malicious attackers to steal sensitive personal information.

Submitted	12 August 2019
Applicable Law	UK
Topic	Data Protection & Privacy Dispute Resolution - Commercial Dispute Resolution - Financial Markets
Contact	Bryony Couchman

A researcher from Oxford University has sent a fake subject access request to over 150 companies in order to prove how the “right of access” under Article 15 of the GDPR can be easily exploited by malicious attackers to steal sensitive personal information.

Using publicly accessible information of his fiancé, together with a fake email address, James Pavur demonstrated that nearly 1 in 4 UK and US based firms willingly provided highly sensitive personal data with little or no verification as to the identity of the individual making the request.

In total, over 60 distinct instances of personal information were disclosed, including highly sensitive information such as the individual’s US social security number, credit card details, home address, and various account usernames and passwords.

The unsophisticated nature of the attack (consisting of a template letter and a simple python mailer script) demonstrates the relative ease in which malicious attackers could successfully steal individuals’ identities on a mass scale. Organisations should therefore be alive to the risk of illegitimate subject access requests such as these, ensuring they have strict identity verification procedures in place, and that these are closely followed. At the very least, methods such as:

1. streamlining SARs through a dedicated online form
2. requesting verification from a previously known email address of the individual, or
3. requiring the individual to login to their existing online account

could considerably reduce an organisation’s vulnerability to such an attack and prevent the organisation being fined - up to €20m or 4% of its annual turnover - for the inadvertent disclosure of personal data.

Pavur and Casey’s full working paper, together with the fake SAR template letter, can be accessed in full here.

elexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS