Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

By email only: hannah.gurga@ukfinance.org.uk

19 May 2021

Dear Hannah,

RE: Use of Behavioural Biometrics in Strong Customer Authentication (SCA)

I write regarding your letter of 1 March that seeks to progress the ICO and UK Finance's considerations of behavioural biometric solutions, as a means of Strong Customer Authentication ('SCA'), under the second Payment Services Directive ('PSD2').

Please be advised that after initial consideration, James Dipple-Johnstone has passed this matter to me, as Executive Director of Regulatory Futures and Innovation, to respond to you.

Background

It is my understanding that the ICO's Relationship Management Service has been engaging with UK Finance's Privacy and Data Ethics division. This engagement has aimed to clarify the financial sector's queries relating to the implementation of behavioural biometrics as a solution for two-factor authentication requirements under SCA.

In January, UK Finance provided the ICO with a positioning paper regarding this issue. In response, the ICO requested further detail and clarification over some of the points raised. It is my understanding that UK Finance recently provided the additional information and you are now looking for the ICO to conclude considerations.

The main question outlined within the positioning paper, and your letter of 1 March, is whether the processing of behavioural biometric data in the context of SCA can meet the 'substantial public interest' requirements for processing under Article 9(2)(g) of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

UK Finance has requested that the ICO provides a steer to determine if

behavioural biometric data, specifically used in this way, can meet the requirements of the Art 9(2)(g) condition. UK Finance has also suggested that without such a steer, there are concerns that many actors within industry will put their solutions on hold, which is problematic within the context of an enforcement date of 14 September 2021.

Our view

The ICO recognises the need for clarity on how it interprets the UK GDPR and DPA 2018 in this context, and we are happy to provide this, below.

That said, UK Finance members looking to implement any behavioural biometric solutions for customer authentication purposes are controllers for that processing and will need to be responsible for their own data protection obligations, based on their own circumstances and after careful consideration of the technologies they wish to implement.

In detail

As identified within the positioning paper; where the requirements of PSD2 and SCA involve the processing of special category data, as defined by the UK GDPR, the relevant conditions from Article 9 that could apply would be explicit consent under Article 9(2)(a) or substantial public interest under Article 9(2)(g).

The positioning paper makes the case for applying the substantial public interest condition, and we acknowledge that this is a possible solution (when the full requirements of the condition are met). Applying the condition is considered to be permissible where there are provisions in domestic law that address the proportionality of the processing in relation to its aim, and contain appropriate safeguards for data subjects. In the UK, such provisions are contained in Schedule 1 of the DPA 2018. The position paper identified paragraphs 10-12 of Schedule 1 as those most relevant to the processing in question.

The ICO acknowledges that such grounds would be appropriate for the use of biometrics for SCA, if controllers carrying out such processing are able to demonstrate that the processing is "necessary" both for the particular purposes set out in those paragraphs 10-12 and for reasons of substantial public interest. This means that this use of biometrics must be a targeted and proportionate way of delivering the specific purposes set out in those paragraphs (such as for preventing or detecting unlawful acts) and for reasons of substantial public interest, and that it cannot be achieved in a less intrusive way.

While UK Finance has explained the advantages of behavioural biometrics over knowledge based methods of authentication, we recommend that this point is considered in more detail by UK Finance members when choosing to implement behavioural biometrics for SCA. In particular, the necessity point would benefit from an analysis of whether, and if so the extent to which, behavioural biometrics provide better protection against fraud and social engineering as compared not only to knowledge based methods of authentication but also as compared to other forms of biometric authentication.

We also recommend that UK Finance and its members consider how the proposed behavioural biometrics would benefit the public, including in practical terms of both depth (the improvements brought about result of the new SCA) and breadth (the volume of people benefiting from the processing).

Ultimately, controllers looking to implement behavioural biometric data as part of SCA requirements must ensure that the rationale for the processing is well considered and the specifics of the processing are justifiable, with a data protection by design approach adhered to.

Such an approach should consider what steps can be taken to minimise the processing of special categories of data, particularly in the context of any data processed by or in conjunction with third parties.

Conclusion

The engagement between UK Finance and the ICO, as well as the subsequent positioning paper has been helpful in understanding the challenges industry is facing as it looks to implement appropriate measures under the SCA requirements of PSD2, before the September enforcement date.

Whilst it is for each individual UK Finance member, as controller, to reach their own determination, the ICO has not uncovered any significant technology policy issues in considering UK Finance's positioning paper or as part of the ICO's wider assessment of behavioural biometrics. This suggests that relying on Article 9(2)(g) is appropriate for the proposed processing.

UK Finance's members will likely need to undertake a Data Protection Impact Assessment ('DPIA'), and/or produce an 'Appropriate Policy Document', with evidence of data minimisation and transparent data processing considered. Additionally, controllers should pay close attention to the principle of

accountability. A controller's record keeping should be clear regarding the necessity for the processing of personal data.

In conclusion, it is recommended that any UK Finance members looking to implement behavioural biometric solutions under the substantial public interest conditions set out in Schedule 1 of the DPA 2018 clearly identify why other bases for processing, such as consent, are inappropriate and clearly and thoroughly assess the necessity of the use of behavioural biometrics for the specified purposes laid out in the relevant paragraphs (10-12).

Yours sincerely,

Stephen Bonner
Executive Director of Regulatory Futures and Innovation