



Worldpay request for Board Member data

28/03/2024

Background

Worldpay requested information (name, address, DOB, nationality) about the Principal and Vice Principal Operations, which was duly provided by Glasgow Kelvin College. They have now requested the same information about the Board of Management (20 members) and Board Secretary. The college believe this is disproportionate as these unpaid/voluntary members have no “significant control” on an individual basis and have no access to the College bank accounts. Worldpay have abruptly withdrawn their service as they have not received the requested information.

Does data protection law apply?

Data protection law applies, specifically ‘data minimisation’ as outlined under UK GDPR Article 5(1)(c):

‘personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.

The request from Worldpay relating to all 20 Board Members and Board Secretary seem excessive and is the grounds upon which the college is disputing the data sharing. The actual data requested (name, home address, DOB, nationality) is minimal. However, it is questionable whether this is necessary given they are not involved in issuing transactions independently nor signatories for the transactions and/or account. **The college is within its rights to challenge this request for personal data.** Indeed, the FIS Security Statement from WorldPay stipulates that the client is responsible for ensuring client personal data is ‘... *minimal, and not excessive*’.

In terms of their privacy notice, Worldpay state that for its payment products, it is an independent Data Controller. This means it determines the purpose and means of the personal data processing and are ultimately accountable for this. Worldpay is transparent about the need for the personal data they request from clients, addressing the UK GDPR principles (see Annex A) including the purposes for which it will be used, specifically:

‘We have an obligation to act in compliance with applicable laws and regulations and to prevent fraud, money laundering and financing terrorism’.

I have written to Worldpay to request clarification on:

1. What Worldpay classes as 'significant control' (this is within emails the organisation has received, with an asterisk beside it, but no footnotes, etc).
2. What is driving the request for personal information on all Board Members rather than signatories/those named on the account.
3. If regulations underpin this request, could you advise what they are and what jurisdictions they cover.
4. If the organisation was to provide the requested information for all Board Members, would this affect the individuals in terms of their personal finance and, if so, how.

What are the risks associated with sharing the data?

Overall, it is my opinion that the data protection risks to the college of sharing these data are minimal. In terms of ‘data minimisation’, the requested data items meet this principle; *adequate, relevant and limited to what is necessary* for regulatory requirements and necessary due diligence. The issue is that it appears

excessive in relation to requesting this information from all 20 Board Members and the Board Secretary when they are not involved in issuing transactions independently nor signatories for the transactions and/or account. The financial sector is highly regulated and there is a need for these organisations to limit their liability, which is why I believe Worldpay are requesting this information. Therefore, on-balance, I do not believe the request is unreasonable.

The risk to the college associated with sharing Board Members data is limited. I believe it is unlikely that the Information Commissioner's Office would take regulatory actions against the college in relation to the sharing of this data, even if they had concerns that it did not meet the 'data minimisation' principle.

The biggest (business) risk to the college is that not sharing the data will result in the withdrawal of Worldpay services.

What can we do?

The college has two options:

- Provide the data requested by Worldpay about your Board Members. This will allow you to continue using their services.
- Refuse to provide the requested data from Board Members to Worldpay and try to work with Worldpay to address your concerns. Failing this, change service provider.

DPO Advice

My advice is to challenge the request, which the college has done. Worldpay have not been receptive to working with the college to address their concerns. As Worldpay state that for its payment products, it is an independent Data Controller, the college is limited in what it can do. The college needs to decide whether to share the data as requested or not. I do not believe the college is at risk of data protection regulatory action regardless of which decision it makes. This will ultimately be a business decision for the college.

Mairead Wood
Head of Data Protection & Governance Share Service,
HEFESTIS

Data Protection (UK) Assessment

Based on the information accessible via Worldpay's Privacy Centre - <https://www.worldpay.com/en-gb/privacy>

1.	Lawfulness, fairness and transparency	• Lawfulness – bases include contract, legal obligation, LI, consent – depends on the processing. Most of the processing for the college will be done under contract and legal obligation. • Information in the Privacy Centre appears fair and transparent. There is a section on 'Clients' under 'Additional Notices' on their website (see below table).
2.	Purpose limitation	• Assembling, maintaining, and disseminating e.g. Client directories, identification credentials, internal record-keeping and reporting, including reporting on credit and financial risk • Supporting, monitoring, auditing, executing, and facilitating: Business negotiations and transactions (including due diligence) • Complying with: Applicable laws and regulations and industry requirements, including reporting and disclosure obligations. • Conducting: Audits and accounting, financial and economic analyses (including to assess financial and insurance risks) • Preventing, detecting, and assisting in the prevention, detection or prosecution of: Crime, including fraud, sanctions offences and money laundering • Processing and administering: Tax and other required withholdings [See info re. clients below this table]
3.	Data minimisation	• Personal data to be processed should be limited to what is needed to meet the purpose for which it was collected. It does seem excessive to request information on all 20 Board Members, however, given the purposes in relation to financial regulations that the data is being used for, it is likely to be needed. This is highlighted above and in the 'client' notice below. SEE ALSO FIS SECURITY STATEMENT (5.).
4.	Accuracy	• Ensure data provided is accurate and up-to-date.
5.	Storage limitation	• Limited information on data retention. Most requirements are likely to be determined by law, and some will fall under their broad term of 'legitimate business need'.
6.	Integrity and confidentiality - security	• FIS Security Statement - there is a statement within this on Data Minimisation - 7. DATA MINIMIZATION Client is responsible for verifying Client Data, including Client Personal Data, provided to FIS for processing or other

		purposes under the Agreement is accurate, current, adequate, of appropriate quality, relevant, minimal, and not excessive. https://www.fisglobal.com/-/media/fisglobal/files/PDF/policy/Solutions/FIS-SECURITY-STATEMENT-v-2023-January.pdf
7.	Accountability	See above re. data minimisation in FIS Security Statement.

Additional Notices – Clients

If you sign up to become one of our clients by entering into an agreement with FIS, we will collect information we need to establish and perform a contract with you, including your contact information, address, ID documentation, tax information and payment details.

We use this information to set up our products and services for you, including providing you with access to our Client Portal. In addition, we use your information for our legitimate interest of managing our internal administration and for complying with our legal obligations, such as know-your-client and anti-money laundering obligations and taxation obligations...

... We have an obligation to act in compliance with applicable laws and regulations and to prevent fraud, money laundering and financing terrorism. As we are active in the financial sector, we are not allowed to accept just any client without checking them and we have to determine and report when suspicious transactions take place. Therefore, if you are applying to become one of our clients and during the performance of our agreement, we will need to collect up to date information and documents to:

- Verify your identity;*
- Identify the ultimate beneficial owners of your business;*
- Identify the purpose and intended nature of your future business relationship with us;*
- Monitor your behaviour and transactions across the FIS solutions using automated systems which detect risks and verify the origins of your capital/assets;*
- Check whether a natural person representing you is competent to do so (and verify the identity of this person); and*
- Check whether you act on behalf of yourself or on behalf of a third party.*

To carry out the above checks, we process the information (including personal data) that you have provided to us and other information created by your use of the FIS services. Which may include your name, your contact information, a copy of your identification document, your tax identification number (if legally required), the address of your legal representative and shareholders, your bank account number, information contained in correspondence between us, bank statements, your signature and an extract of your company registration document. We use third party identification and verification services (including credit reporting agencies) in order to assist us to verify your identity and the documents provided to FIS.

Legal grounds for processing personal data of clients are:

<i>Performance of a contract</i>	<i>Article 6.1.b GDPR Article 13.(2) PIPL</i>
<i>Compliance with a legal or regulatory obligation, including know-your-client, anti-money laundering and taxation obligations</i>	<i>Article 6.1.c GDPR Article 13.(3) PIPL</i>
<i>Our legitimate interest in providing you with our goods and services and securing prompt payment of any fees, costs and debts in respect of our services</i>	<i>Article 6.1.f GDPR</i>

<i>Our legitimate interest in responding to questions, queries, comments and complaints you send or share with us</i>	<i>Article 6.1.f GDPR</i>
<i>Our legitimate interest in safeguarding FIS against inadvertently dealing with the proceeds of criminal activities or assisting in any other unlawful or fraudulent activities (for example, terrorism)</i>	<i>Article 6.1.f GDPR</i>
<i>Our legitimate interest in sending you direct marketing communications to keep you informed about our products and services and to invite you for relevant events</i>	<i>Article 6.1.f GDPR</i>