PCS GROUP
TRANSFER IMPACT ASSESSMENT

1 BACKGROUND TO & PURPOSE OF THIS TRANSFER IMPACT ASSESSMENT

1.1 This Transfer Impact Assessment (**TIA**) has been prepared in response to the Schrems II decision and the EDPB Recommendations and for the purposes of clauses 14(a) and 14(c) of the EU Standard Contractual Clauses, and equivalent provisions in the United Kingdom. It provides an assessment of whether the laws or practice of a third country where we process customer data impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools.

1.2 This TIA focusses on outlining our analysis of the local laws of the third countries to which Personal Data is transferred; principally the United States of America (the "**US**"). This TIA then considers the impact those laws have on the effectiveness of the protection measures implemented by us and our customers in connection with the protection of Personal Data transferred between them.

1.3 Where any risks have been identified, this TIA provides details of the appropriate supplementary measures which we implement to mitigate these risks, and to help ensure the level of protection afforded by EU and/or UK law standards are maintained. In addition to fulfilling our data protection obligations, this TIA will assist our customers with their own due diligence obligations as data controllers/data exporters.

2 SUMMARY OF OUR PROCESSING

2.1 We process personal data for the following purposes:

2.1.1 For past, present and future employee personal data:

2.1.1.1 managing internal and external disputes;

2.1.1.2 day-to-day helpdesk queries;

2.1.1.3 employee on-boarding;

2.1.1.4 employee communications;

2.1.1.5 administration of payroll, health insurance and pensions;

2.1.1.6 travel organisation;

2.1.1.7 risk assessments; and

2.1.1.8 equal opportunities monitoring,

(together the "**Employee Processing Purposes**").

2.1.2 For prospective, current and previous customer personal data:

2.1.2.1 review of customer contracts;

2.1.2.2 customer on-boarding and communications;

2.1.2.3 verification of identification and running ID checks against criminal database;

2.1.2.4 facilitation and support for the trade-in programme;

2.1.2.5 processing of trade-in devices received from individuals; and

2.1.2.6 trade-in kit fulfilment and payment,

(together the "**Customer Processing Purposes**").

2.1.3 For prospective, current and previous commercial partner personal data:

2.1.3.1 review of supplier contracts;

2.1.3.2 logistics management; and

2.1.3.3 scoping out future integrations with trade-in partners,

(together the "**Partner Processing Purposes**").

2.2 Outside of the EU and UK, we will process this personal data in the US to manage the processes enable the purposes mentioned above. The data flows are:

- UK → US
- EEA → US

3 SUMMARY OF LOCAL LAW ASSESSMENTS

In this section, we have summarised the legislation it has considered in this TIA below. A more detailed overview of the relevant legislation considered is set out in Schedule 1 of this TIA.

Territory	Legislation considered	Does this legislation undermine the protection afford to data subjects? If not, why?	Have we ever received a request from a public agency in connection with this legislation?
US	The Wiretap Act	In our view, no. The potential for data subjects having fewer rights and mechanisms of redress in the US under equivalent data protection frameworks in the UK and EU is noted in connection with the more detailed review of local laws set out in Schedule 1. Our adoption of the standard contractual clauses (SCCs) and the UK Addendum to the SCCs, and the application of these data transfer provisions to onward transfers significantly mitigates these risks. Further, the nature of the data we process as described in this TIA is unlikely to be of value or interest to relevant government bodies. The data we process is also protected by substantial security measures as set out in section 4 of this TIA. We also note the following comments on the US security laws provided by US government bodies in connection with Schrems II: *As a practical matter, for many companies the issues of national security data access that appear to have concerned the ECJ in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community… Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies.*	No
US	The Stored Communication Act		No
US	Foreign Intelligence Surveillance Act		No
US	Executive Order 12333		No
US	Subpoenas generally		No

4 APPLICATION OF TRANSFER IMPACT ASSESSMENT GUIDANCE TO OUR BUSINESS

Please refer to the PCS Wireless Technical and Organisational Security Measures Summary, a copy of which is included in the Annex to this TIA.

5 OTHER SPECIFIC TOPICS OF RELEVANCE TO THIS TIA

Extent to which data is accessed in the clear outside of the UK and EEA:

We understand the importance of protecting personal data from unauthorised access. We also understand the guidance set out by the European Data Protection Board following the Schrems II case. This guidance requires the data controller to understand the extent to which access may take place outside of the UK and EEA to data which is un-encrypted or in the clear.

We operate a global business and will transfer personal data relating to data subjects in the UK and EEA to our own systems in the US and which may then be transferred to processors in the US for the purposes of conducting the Employee Processing Purposes, the Customer Processing Purposes and the Partner Processing Purposes.

Likelihood of risk associated with data which is accessed in the clear outside of the UK and EEA:

Risks

The following factors are relevant to this risk assessment:

1. The Personal Data being processed

We process the following personal data:

- *Name*
- *Email address*
- *Telephone number*
- *Fax Number*
- *Address*
- *Health Information*
- *Salary Details*
- *Grievances (appraisals and performance)*
- *Device IDs and IMEIs*
- *Criminal record*
- *Bank Details*
- *EORI number*

- *ID: passport / driving licence*
- *Emergency Contact*
- *CV*
- *Social Security / NI Number*
- *Date of Birth*
- *Marital Status*
- *Gender*
- *Passport Number*
- *Ethnic origin*
- *Sexual orientation*
- *Religion or belief*
- *Vehicle licence plates*

2. The risk a foreign government could compel us to disclose personal data

We have conducted a risk assessment to evaluate the risk of a foreign government making an intelligence related request for customers' personal data.

This jurisdiction in which this could take place is the US.

United States

We will transfer employee and customer data to third parties in the US for the purposes of conducting the Employee Processing Purposes, the Customer Processing Purposes and the Partner Processing Purposes.

The US has several items of legislation that may compel an employee to provide access to data in the clear on behalf of the intelligence authorities of the United States. This includes the laws identified in this TIA, including FISA 702, and Executive Order 12333, as limited by Presidential Policy Directive 28.

For the intelligence agencies to compel us to disclose one of the data types above, the US government agency must contact a US employee and compel them not to inform any non-US management.

It is also necessary for there to be a compelling reason for a US intelligence or National Security authority to request personal data that a customer has submitted to the platform. It is assessed that the customer data we hold are likely of limited interest to the US intelligence authorities as these data items can be either easily deduced by examining public records of the customer's business or the relevant individual. It is assessed that there would be limited advantage to the US intelligence or government authority in requesting this information from us directly.

Overall, it is assessed that there is limited benefit in a US authority in requesting such information and as such we would assess the risk of being asked to provide such data as being extremely low.

At this time we have not received any national security letter, or any other instruction from US intelligence or government authorities to provide our customers' data. We will remove this statement from a published version of this document should this cease to be the case and issue a new version of this document as soon as such a request is made.

Risk Minimisation

Relevant PCS entities making or receiving transfers of personal data from the UK and / or EEA to a third country have signed an Intra-Group Data Processing Agreement setting out key obligations to ensure personal data is protected by equivalent measures as it would be in the UK or EEA.

History of requests for access to personal data from any security or public authority to date:

None

6 CONCLUSION

6.1 For the reasons set out above (and particularly section 3 of this TIA) we conclude that its current processing activities can continue.

6.2 We will review this TIA periodically (at least annually). We will review and update this TIA in the event: (i) a new processing location is used to process customer data; or (ii) it becomes aware of a change in local applicable law in an existing processing location which may impact the conclusions drawn in this TIA.

SCHEDULE 1

THIRD COUNTRY SUMMARY OF LOCAL LAWS: UNITED STATES OF AMERICA

Are there laws which establish the rule of law and which protect human rights and fundamental freedoms?

The United States Constitution and Bill of Rights provide broad civil rights protections. For example, the First Amendment of the US Constitution protects the right to free speech, to peaceful assembly and to petition the government for redress, the Fourth Amendment protects against unreasonable search and seizure by the government (which has been construed to generally require a warrant for surveillance of electronic communications, outside the context of foreign intelligence activities directed outside the United States), the Fifth Amendment provides the right to due process of law and the right not to be compelled to incriminate oneself, the Sixth Amendment provides for a trial by jury and the right of confrontation, and the Eighth Amendment protects individuals from cruel and unusual punishment. In addition, the US Supreme Court has identified fundamental rights not explicitly stated in the Constitution, such as the presumption of innocence in a criminal trial rebuttable only by proof beyond a reasonable doubt. The United States Congress has also passed many various laws that protect individual freedoms in the privacy context, some of which specifically impose limitations on government search or surveillance of data, as discussed below.

What are the laws regulating public authority surveillance of personal data held by private organisations?

The United States has various federal and state laws that regulate electronic surveillance and protect privacy rights in that context. The key federal laws are as follows:

Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§ 2510-2522) Title III, also known as the Wiretap Act, broadly prohibits the interception and disclosure of wire, oral and electronic communications, as well as the manufacture, distribution and possession of such interception devices. At the same time, it establishes a detailed regulatory regime under which federal and state government authorities may, in certain criminal investigations, intercept, disclose and use such communications as evidence. Originally the Act only applied to 'oral' and 'wire' communications but the Electronic Communications Privacy Act of 1986 ('ECPA') broadened the application of the statute by expanding the kinds of communications to which the statute applied to also cover 'electronic' communications. Where it applies, the statute requires law enforcement authorities to obtain a judicial order authorising interception of oral, wire, and electronic communications, based on a showing of probable cause that particular communications evidencing one of the crimes covered by the statute (consisting of serious felonies) will be obtained through the intercept. This requires a 'full and complete statement of the facts and circumstances,' including 'details' underlying the alleged offense and a 'particular description' of the nature and location of the facilities or place to be wiretapped, the types of communications to be intercepted, and the persons committing the offense and whose communications are to be intercepted. The application must also contain a 'full and complete statement' describing all other investigative techniques that have been tried and failed or explaining why such techniques are likely to be unsuccessful or too dangerous. The court must determine, prior to granting the order, that 'normal investigative procedures' have been or would be unsuccessful

or excessively dangerous. The government's application must also show that the surveillance will be conducted with procedures in place to minimise the interception of communications irrelevant to the investigation.

Stored Communications Act (18 U.S.C. § 2701 - 2712) Title II of the ECPA is the Stored Communications Act ('**SCA**'). Whereas the Wiretap Act applies to the live interception of communications, the SCA applies to the collection of stored communications maintained by third-party service providers. The SCA generally prohibits the unauthorised access of a facility through which an electronic communication service is provided. It also sets forth requirements that law enforcement authorities must meet in order to require a third-party service electronic communications or remote computing service provider to disclose stored electronic communications. In this regard, the SCA generally requires law enforcement authorities to obtain a search warrant in order to compel such a provider to disclose the contents of stored electronic communications.

Foreign Intelligence Surveillance Act (15 U.S.C. § 1681) ('**FISA**') establishes standards and procedures for conducting electronic surveillance for foreign intelligence purposes in the United States. FISA can be used when foreign intelligence is a 'significant purpose' of the investigation and orders permitting surveillance are issued by the Foreign Intelligence Surveillance Court ('**FISC'**). Surveillance methods include wiretaps, pen register, trap and trace and video surveillance. For foreign intelligence surveillance directed at persons within the United States, FISA generally requires authorities to obtain a judicial order authorising the surveillance, similar to the type of order required under the Wiretap Act, except that instead of showing that there is probable cause to believe that the surveillance will yield evidence of a crime, the government must show probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power (which can include a foreign terrorist group).

FISA was not originally intended to apply to foreign intelligence surveillance activity directed outside the United States, which traditionally was done through interception of communications transmitted via satellite or undersea cable. In 2008, FISA was explicitly amended to authorise intelligence authorities to conduct foreign intelligence surveillance of non-US person targets located outside the United States by compelling electronic communications service providers to disclose the communications of such a target. While this authority does not require individual warrants issued by the FISC (since the targets of such surveillance are not US persons and as such are not protected by the Fourth Amendment of the US Constitution), the exercise of this authority is nonetheless subject to multiple layers of oversight from the executive branch, the FISC (made up of independent judges), and congressional intelligence committees alongside multiple levels of internal review and technological controls over access to the data. It is also subject to Presidential Policy Directive 28 ('PPD-28'), an executive directive that requires signals intelligence activities to be 'as tailored as feasible.'

Cloud service providers fall specifically within the scope of Section 702 of FISA, which provides that information must be acquired from an electronic communication service provider, including remote computing service providers that provide computer storage or processing services to the public. The DNI, DOC, and DOJ jointly produced a whitepaper (Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II) discussing factors that companies should consider in their assessment of post-Schrems compliance with SCCs, specifically discussing the safeguards in place for those transferring personal data from the EU to the U.S. Of particular note, the whitepaper states:

"As a practical matter, for many companies the issues of national security data access that appear to have concerned the ECJ in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community… Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies."

Reference was made in the Schrems II case to Executive Order 12333 ("EO12333"). EO12333 assigns the different U.S. intelligence agencies responsibilities related to clandestine intelligence collection and places restrictions on certain agencies' activities. EO 12333 does not authorize the U.S. government to require any company or person to disclose data, including data transferred under SCCs. The whitepaper suggests that there is little to no concern with EO12333 as it relates to complying with the new SCCs.

What legal bases/purposes are there for public authorities to access personal data held by private organisations? Are these bases/purposes exhaustive or do public authorities have general discretion?

Law enforcement authorities in the US, like law enforcement authorities in many countries, have the authority to issue subpoenas to persons or companies for records in their custody, possession, or control that are relevant to a pending law enforcement investigation. Such records may include personal data. For example, it is common in law enforcement investigations for authorities to subpoena a person's telephone call records or bank records, which may contain personal data.

With respect to various specific types of information, there are heightened requirements in place. Most importantly, as indicated above, with respect to the content of communications, the government generally cannot intercept such communications or compel a third-party communications provider to disclose such communications without an appropriate judicial order or warrant, based on a showing of probable cause to believe that the interception or disclosure will yield evidence of a crime.

What other limits, such as limits to scope or retention periods, are there to the actions of public authorities?

Generally there are no specific retention periods required by statute. However, agencies may impose their own retention limits. Moreover, under the Fourth Amendment, any electronic search or surveillance must be conducted in a reasonable manner, meaning that law enforcement agents must tailor the scope of their search or surveillance based on what is relevant to the investigation.

Has an independent supervisory authority been established which provides oversight for the protection of privacy, and what is their role?

The courts are the primary mechanism for oversight of privacy protections, particularly in the criminal context.

What are the oversight mechanisms for the approval and review of relevant actions by public authorities? Are there oversight mechanisms in place for when actions by public authorities are conducted in secret?

As described above, for searches or surveillance of electronic communications, generally a warrant or judicial order is required, which must be approved by a neutral magistrate judge. Moreover, in the event that evidence gathered through such searches or surveillance is used as criminal evidence against a person, the person may challenge the admissibility of the evidence - including challenging the validity of the warrant or judicial order - if it was obtained in an unconstitutional or otherwise unlawful manner.

US laws also provide electronic communication service and remote computing service providers with a mechanism to challenge orders compelling disclosure of customer communications. Both the SCA and the FISA contain such provisions. In addition, the USA Freedom Act brought more transparency to government surveillance activities, including by requiring reporting certain information to Congress and the public each year and requiring FISC to make their orders publicly available if they were deemed to address any novel Fourth Amendment legal interpretations. Additionally, the Act allows companies to issue more detailed data about the demands for user information that they receive from the government. For instance, a number of organisations now release an annual transparency report indicating a range of national security letters ('NSLs') and other information requests they have received from the government.

Are there legal remedies for data subjects?

As above, the courts are the primary mechanism for oversight of privacy protections in relation to actions by public authorities. In the criminal context, criminal defendants may challenge the admissibility of evidence on the basis that the surveillance or other method of obtaining such information was unconstitutional or otherwise unlawful.

Additionally, US law also provides various ways in which individuals can sue the government or individual government officials if they have been harmed by search or surveillance activity that is unconstitutional or unlawful, although such lawsuits can be limited by various sovereign or official immunity doctrines, depending on the facts.

Can an organisation refuse to comply with a request and what remedies are available to them?

Yes, any organisation served with a warrant, subpoena or other form of legal process requiring disclosure of a customer's data may seek to challenge the legitimacy of the order and seek to quash it in court if it believes the order is somehow unlawful. In particular, an organisation may challenge such process on the ground that it would require them to violate foreign data privacy laws. In the face of such a challenge, if the court finds there to be a true conflict of laws, the court will apply a balancing test that weighs the US interests in enforcing the process against the interests of the foreign sovereign.

Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects? If not, what are the differences?

The US Constitution does not apply to non-US citizens outside the United States and therefore the protections in the Fourth Amendment do not apply to non-US citizens abroad.

FISA, which specifically permits foreign intelligence surveillance of non-US persons located outside the US, provides for multiple layers of oversight from the executive branch, the FISC and congressional intelligence committees. Additionally, through PPD-28, the executive branch has extended some limitations designed to ensure that even signals intelligence activity directed towards non-US citizens abroad is as tailored as feasible, taking into account the availability of other sources of information.

Has the jurisdiction entered into international commitments, such as legally binding conventions or instruments related to data protection? For example, Convention 108.

The United States has Mutual Legal Assistance Treaties with a number of countries including the United Kingdom and every member of the EU. It is also a member of the Budapest Convention on Cybercrime which serves as a framework for international cooperation between parties to the Convention regarding the exchange of evidence and information in cybercrime-related matters, including electronic data. The United States has a CLOUD Act Agreement with the United Kingdom which makes it easier for American and British law enforcement agencies, with appropriate authorization, to obtain electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from communication providers / technology companies based in the other country.

ANNEX

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES SUMMARY

Security measure	**Details**
Measures of pseudonymisation and encryption of personal data	• Data is encrypted whilst in transit. • Data is pseudonymised wherever practicable when recorded on internal systems or shared with third parties.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, and for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures	• We conduct regular IT security reviews to ensure best practices are adopted. • Contracts with third parties requiring robust security mechanisms when processing personal data.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Regular back-ups made of personal data. • Mirroring of hard disks. • Uninterrupted power supply. • Firewalls. • Regularly updated disaster recovery plan.
Measures for user identification and authorisation to prevent unauthorised users from accessing data	• We adopt two-factor authentication where appropriate. • Password protection of documents containing sensitive personal data. • Automatic lockout for inaccurate passwords. • Access rights dependent on the necessity of accessing the data based on roles.
Measures for the protection of data during transmission	• We undertake penetration tests to check that data in transit is fully protected. • We ensure safeguards are in place for any international transfers of personal data to our subprocessors and other relevant parties, usually using the EU Standard Contractual Clauses with the UK Addendum.
Measures for the protection of data during storage	• We encrypt data at rest to ensure data is not written to storage in unencrypted

Security measure	Details
	form. • We adopt password protection and controls on user access where appropriate.
Measures for ensuring physical security of facilities at which personal data are processed	• Entry to our building is protected by physical and digital security measures including smart cards and surveillance systems. • Our servers and communications hardware are located in a secure server room. • We ensure products containing personal data are securely managed with inbound collection and reception of equipment into PCS owned and operated facilities, ensuring chain of custody.
Measures for ensuring events logging	• Our systems permit us to see an audit trail of changes to documents by personnel.
Measures for ensuring system configuration, including default configuration	• Any new systems our assessed by our IT security team prior to implementation.
Measures for internal IT and IT security governance and management	• We maintain our IT security and review our practices periodically to ensure the measures are appropriate for the size of our organisation and the type of personal data we handle.
Measures for certification/assurance of processes and products	• We seek advice from external legal counsel to ensure we are aware of our obligations under the data protection legislation. • We hold ISO certification for Quality Management Systems & Processes (ISO-9001-2015) and Environmental Management Systems & Processes (ISO-14001-2015).
Measures for ensuring data minimisation *Measures for ensuring data quality*	• We only collect the data needed to provide our services. • We have strict policies requiring customers using our trade-in offering to delete all personal data from devices before sharing them with us. In the event of user error, we utilise Asset Science (see below) to remove remaining data.
Measures for ensuring limited data retention	• We use a data clearing method from Asset Science, which has been ADISA certified to remove data from trade-in devices. • We adhere to an internal data retention policy reviewed by external legal

Security measure	Details
	counsel.
Measures for ensuring accountability	• Data that is collected for different purposes is processed separately. • We maintain separation between our business units and group entities where appropriate. • We have a robust Intra-Group Data Sharing agreement that sets out responsibilities and requirements for processing data.
Measures for allowing data portability and ensuring erasure	• We require all employees to adhere to a robust Data Protection Policy, which includes set procedures to follow in the event a data subject exercises their rights to erasure, access, portability or any other rights. • We hold up to date Article 30 Records of Processing activities that record how data is held within our business.