Ahern Rudden Quigley
Solicitors
5 Clare Street
Dublin 2

T +353 (0) 1 661 6102
E enquiries@arqsolicitors.com
W www.arqsolicitors.com
DX 162 Dublin

AHERN
RUDDEN
QUIGLEY

Our Ref: **GR/MC/SCH002-9341** Your Ref: Date: **5 August 2020**

Mason Hayes & Curran
South Bank House
Barrow Street
Dublin 4

BY EMAIL ONLY:
[redacted]

Re: DPC -v- Facebook Ireland Limited and Maximilian Schrems
Your Client - Facebook Ireland Limited
Our Client- Maximilian Schrems

Dear Sirs,

We refer to the above.

Article 13(1) GDPR provides as follows:

"Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

> *(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."*

Article 30(1)(e) GDPR provides as follows:

"Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

> *(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards"*

Clause 4(h) of the Annex to Commission Decision 2010/87/EU provides as follows:

"The data exporter agrees and warrants:

> *(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;"*

On behalf of our client, we request that your client clarify, by close of business on Friday 7 August 2020, the precise named recipients and the legal basis that Facebook Ireland Ltd relies on for the EU-US data transfers of our client's personal data, as well as furnish a copy of the current SCCs and/or any other agreement or supplementary agreement your client may use. Your client is obliged to provide this information pursuant to Article 13(1)(f), 14(1)(f) and 15(1)(c) and (2) GDPR and the relevant clause of the SCCs.

Should you have any information that would lead your client to believe that Facebook Inc. is not subject to 50 USC § 1881a and/or EO 12.333 or if you seek to rely on any other measure, legal argument or document that would make continuous data transfers to Facebook Inc. legal despite the clear findings by the CJEU in C-311/18 Schrems paras 150 to 202, please furnish us with details.

We look forward to hearing from you.

Yours faithfully,

Ahern Rudden Quigley

Ahern Rudden Quigley

Email: [redacted]

MASON
HAYES &
CURRAN

Barrow Street
Dublin 4, Ireland
D04 TR29
DXII Dublin
+353 1 614 5000
dublin@mhc.ie

Ahern Rudden Quigley
Solicitors
5 Clare Street
Dublin 2

BY EMAIL ONLY - [redacted]

19 August 2020 **Your ref:** GR/MC/SCH002-9341 **Our ref:** CMO/AYN/37079.783707978

MHC-23083970-123071888-1

Matter: DPC –v- Facebook Ireland Limited & Maximillian Schrems
Our client: Facebook Ireland Limited ("FIL")
Your client: Maximillian Schrems

Dear Sirs

We refer to your letter dated 5 August 2020 in which you ask a number of questions on behalf of your client relating to data transfers by FIL. As outlined in our initial reply to you dated 7 August last, similar questions were recently sent directly by your client to FIL and FIL has already replied directly to your client in this regard.

In these circumstances, our replies to the questions asked in your letter of 5 August last (which largely consist of a repetition of the replies already sent directly by FIL to your client) are as follows:

1. ***"[...] clarify...the precise named recipients and legal basis that Facebook Ireland Ltd relies on for the EU-US data transfers of our client's personal data..."***

The '*How do we operate and transfer data as part of our global services*?' section of FIL's Data Policy notes "*[we] share information globally, both internally within the Facebook Companies and externally with our partners and with those you connect and share with around the world in accordance with this policy. Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this policy*". The '*How is this information shared?*' section of FIL's Data Policy provides information on the recipients and categories of recipients with which FIL shares personal data in the context of the Facebook service.

The '*What is our legal basis for processing data*?' section of FIL's Data Policy and the legal basis information page note, among other things, that one of core data uses necessary to provide Facebook's contractual services is to "*[t]o transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries*".

2. **"[...] *furnish a copy of the current SCCs and / or any other agreement or supplementary agreement your client may use.*"**

   An extract of the Standard Contractual Clauses entered into by FIL and Facebook, Inc. in relation to the transfer of European region user data is attached.

3. ***"Should you have any information that would lead your client to believe that Facebook Inc. is not subject to 50 USC § 1881a and/or EO 12.333 or if you seek to rely on any other measure, legal argument or document that would make continuous data transfers to Facebook Inc. legal despite the clear findings by the CJEU in C-311/12 Schrems para 150 to 202, please furnish us with details*"**

   The information requested falls outside the scope of the Articles of the GDPR cited in your letter as the basis for this request (and, for the avoidance of doubt, any other provision of the GDPR, as explained by FIL to your client already).

As explained in the *'How do we operate and transfer data as part of our global services?'* section of FIL's Data Policy and as already communicated by FIL to your client, information controlled by FIL will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where your client lives for the purposes described in the Data Policy. These data transfers are necessary to provide the services set forth in the Facebook Terms of Service and to globally operate and provide these services. If your client does not want his personal data to be transferred in the context of providing and operating the Facebook service, he can delete his account at any time by following the steps described under the *'How do I permanently delete my account?'* heading on the following page: https://www.facebook.com/help/224562897555674.

Yours faithfully

Mason Hayes + Curran LLP

MASON HAYES & CURRAN LLP

As per your request, please find an extract of our Model Contract Clauses, which relate to how your data is transferred from the EEA below.

Please note that for the purposes of these Model Contract Clauses, the "data exporter" is **FACEBOOK IRELAND LIMITED**, a limited liability company constituted under the laws of Ireland with an address at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 and the "data importer" is **FACEBOOK INC**, a company constituted under the laws of Delaware with an address at 1601 Willow Road, Menlo Park, CA 94025, California, United States of America.

Model Contract Clauses (Controller to Processor)

BETWEEN

(1) The parties named in the Agreement as a Data Controller shall be the "**data exporter**" in respect of the Relevant Personal Data for which it acts as a controller under the applicable data protection law;

AND

(2) The party named in the Agreement as the Data Processor shall be the "**data importer**";

each a "**party**" and together, the "**parties**",

HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1 Definitions

For the purposes of the Clauses:

"**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**") on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"**the data exporter**" means the controller who transfers the personal data;

"**the data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 45 of the GDPR;

"**the subprocessor**" means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

"**the applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

"**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2 Details of the Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3 Third-Party Beneficiary Clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.2 to 4.9, Clause 5.1 to 5.5, and 5.7 to 5.10, Clause 6.1 and 6.2, Clause 7, Clause8.2, and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5.1 to 5.5 and 5.7, Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5.1 to 5.5 and 5.7, Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4 Obligations of the Data Exporter

The data exporter agrees and warrants:

4.1 that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

4.2 that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

4.3 that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this Schedule;

4.4 that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

4.5 that it will ensure compliance with the security measures;

4.6 that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of the GDPR;

4.7 to forward any notification received from the data importer or any subprocessor pursuant to Clause 5.2 and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

4.8 to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

4.9 that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

4.10 that it will ensure compliance with Clause 4.1 to 4.9.

5 Obligations of the Data Importer

The Data Importer agrees and warrants:

5.1 to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and / or terminate this Agreement;

5.2 that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under this Agreement and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and / or terminate this Agreement;

5.3 that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

5.4 that it will promptly notify the data exporter about:

5.4.1 any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

5.4.2 any accidental or unauthorised access; and

5.4.3 any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

5.5 to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

5.6 at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

5.7 to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

5.8 that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

5.9 that the processing services by the subprocessor will be carried out in accordance with Clause 11;

5.10 to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6 Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with Clause 6.1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in Clauses 6.1 and 6.2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7 Mediation and Jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and / or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

7.1.1 to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

7.1.2 to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8 Cooperation with Supervisory Authorities

8.1 The data exporter agrees to deposit a copy of this Agreement with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to Clause 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5.2.

9 Governing Law

9.1 The Clauses shall be governed by the law of the Member State in which the data exporter of the Relevant Personal Data is established.

10 Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11 Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in Clause 11.1 shall be governed by the law of the Member State in which the data exporter of the Relevant Personal Data is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.10, which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12 Obligation after the Termination of Personal Data Processing Services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and / or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in Clause 12.1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

USER DATA

Data exporter

The data exporter in respect of User Data is Facebook Ireland Limited, a provider of social network products and services to users based in the Territory.

Data importer

The data importer is a provider of advertising, marketing, technical and other support services to the data exporter.

Data subjects

The personal data transferred concern the following categories of data subjects:

- Individuals who visit, access, use or otherwise interact with products and services of the data exporter (including for the avoidance of doubt, Facebook and Instagram).

Categories of data

The personal data transferred is the personal data generated, shared and uploaded by or about individuals who visit, access, use or otherwise interact with the products and services of the data exporter (including Facebook and Instagram).

- information related to the things users do and the information users provide when using the services (such as profile information, posted photos and videos, shared location information, communications between users, and related information about use of the products and services);

- information related to the data subjects that other users of the products and services provide (such as a user's imported contacts or photos);

- information related to users' networks and connections (such as a user's connections to groups, pages, and other users);

- information related to payments (such as information related to purchases or financial transactions);

- information about devices (such as information from or about the computers, phones or other devices where users install software provided by, or that access products and services of, the data exporter);

- information from websites and apps that use products and services of the data exporter (such as information about visits to third-party websites or apps that use a “like” or “comment” button or other service integrations); and
- information from third-party partners (such as information related to jointly offered services or use of third party services); and information from affiliates of Facebook and companies in the Facebook family of companies.

Special categories of data

Such data may include:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation; and
- genetic data and biometric data (as those terms are defined in the GDPR) for the purpose of uniquely identifying a natural person.

Processing operations

Depending on the products and services visited, accessed, or used by the data subject, and subject to any relevant permissions, controls and other internal instructions, the personal data transferred may be subject to the following types of processing activities:

- providing, improving and developing the products and services of the data exporter (such as to personalise content, enable communications between users, make suggestions, conduct surveys and research, customise services based on location, and trouble-shoot issues);
- communicating with users (such as explaining terms and policies, responding to customer services queries, or providing updates about products and services);
- showing and measuring ads and services (such as displaying relevant ads and measuring the effectiveness of ads);
- promoting safety and security (such as using information to verify accounts, investigate suspicious activity or possible violations of terms or policies, or responding to law enforcement, civil law, and other legal requests);
- providing technical engineering support and trouble-shooting;
- activities in connection with the provision of marketing and sales support, including generating reports about the effectiveness of such advertising, identifying issues arising from the delivery and implementation of such advertising; and
- activities in connection with conducting and supporting research and innovation and the development, testing and improvements of products and services.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4.4 and 5.3:

The following information provides an overview of the security measures designed and implemented by the data importer to protect its systems, including the physical, technical, and administrative controls that govern access and use of the data importer's systems.

Technical and Organisational Measures

Within its area of responsibility, the data importer adopts the following technical and organizational measures for processing transferred data.

1 Physical security

Among other measures, the data importer takes the following actions to prevent unauthorized access to equipment processing or using data:

- physical access to Facebook facilities is monitored by guard staff 24x7;
- all individuals must identify themselves to security personnel in order to be admitted to the Facebook premises used by the data importer (or certain areas thereof). This requires a Facebook-issued photo badge with an electronic access code;
- there are documented processes in place for the issuance of Facebook badges; the possession as well as the return of such badges is tracked and verified;
- visitor logs are kept, and visitors receive temporary badges and must be accompanied by a Facebook employee to be admitted to areas beyond the Facebook premises' reception;
- only authorized Facebook employees, vendors, and contractors that work in the Facebook premises are issued access badges for these installations; and
- standard security measures observed, which are typical on Facebook premises, are composed of known technologies and follow generally recognized best practices for the industry, including electronic access systems with card readers, alarm systems, interior and exterior cameras as well as extensive security personnel.

2 Logical access and security

Strict policies are in place to address and limit access to production systems. For certain data access tools, tool owners authorize the nature and extent of access privileges prior to granting access. The procedures for requesting and generating certificates to access data for development and production are documented.

The data importer also takes the following actions to prevent the unauthorized use of data-processing equipment:

- it follows a formal protocol to grant or deny access to Facebook resources. Various access restrictions help to make access secure and limited;

- one-time personnel identification, strong passwords and periodic reviews of access lists are in place to ensure that personnel accounts are put to their intended uses;

- authorized access to internal support tools is controlled by means of a permissions service developed and distributed by Facebook;

- the certificates grant personnel access based on role and is password protected in a restricted system. For certain restricted systems, dual-factor authentication is required;

- unique personnel IDs are used to authenticate to systems;

- passwords are configured to enforce password length and complexity; and

- login history and failures are tracked.

Additionally, the data importer takes the following actions to ensure that the parties authorized to use a data processing system only have access to the data for which they have been specifically cleared, and that stored data or data being processed cannot be read, copied, changed or removed:

- authorization for Facebook services is enforced at all times and at all levels of a given system, with access rights being granted or processed on the basis of the personnel member's job responsibilities / need-to-know, which is provided via workflow tools;

- access to production systems is restricted to trained and specifically authorized personnel members. Such access is revoked in the event of an individual's dismissal or termination of employment;

- the data importer conducts security audits, to ensure vendors follow Facebook security guidelines and sets application and personnel security as key vendor contractual obligations; and

- use of a centralized logging system. Access to the logging system is restricted to authorized personnel and the logs are protected from modification and deletion from non-admin personnel.

3 Technical security

The data importer deploys a range of technical security measures to protect its systems:

- and network traffic are monitored by both industry-standard and proprietary tools to detect and respond to any potential security breaches; and

    - monitoring servers using best-in-class instrumentation tools that log changes to the servers and detect signs of a potential compromise; and

    - using a combination of industry-standard sandboxing technologies and a sophisticated Network Intrusion Detection system to monitor network activity for signs of malicious activity. In addition, a team of security experts continually studies real-world attacks and develops threat intelligence about the attackers' tools and techniques so that security systems accurately detect indications of potential compromise.

- TLS encryption is part of the standard security architecture at Facebook. Core transport services require encryption, such as SSH or HTTPS, to exchange information;
- encryption technology is used to provide security for online user authentication and administrator sessions;
- remote data access to production equipment requires a link to the company's Intranet, which is subject to a dual authentication mechanism;
- a VPN connection is necessary for personnel to access certain internal resources remotely
- changes to the infrastructure and back-end environment, including changes to security tools, follow the Facebook coding and release process;
- all committed code changes are reviewed by an individual that is different than the developer and are tested prior to commit to production
- the data importer uses a firewall configuration policy, which defines acceptable services that may be used in Facebook's environment. Only required ports and services are open. Changes to the firewall configuration are subject to review by the network and security personnel.

4 Organizational security and training

In addition, the data importer provides employees and contractors with education and training on specific technical and organizational security measures.

Facebook employees are required to complete computer-based training on data protection and privacy and security that includes privacy and security by design, vendor security audits, privacy laws and regulations, corporate policies and key privacy principles, and security awareness best practices.

All newly hired employees and contractors are required to complete training in privacy, security, ethics, and confidentiality.

Facebook's security team conducts company-wide security awareness activities to reinforce information security practices and policies.

Ahern Rudden Quigley
Solicitors
5 Clare Street
Dublin 2

T +353 (0) 1 661 6102
E enquiries@arqsolicitors.com
W www.arqsolicitors.com
DX 162 Dublin

AHERN
RUDDEN
QUIGLEY

Our Ref: **GR/MC/SCH002-9341** Your Ref: **CMO/AYN/37079.783707978** Date: **21 August 2020**

Mason Hayes & Curran
South Bank House
Barrow Street
Dublin 4
DX 11 Dublin

Email: [redacted]

Re: DPC –v- Facebook Ireland Limited and Maximilian Schrems
Your Client – Facebook Ireland Limited
Our Client- Maximilian Schrems

Dear Sirs,

We refer to the above and to your letter of 19 August 2020.

As you are aware, a fundamental aspect of processing of our clients data is that our client is aware of that processing and your client has an appropriate legal basis for that processing. In your letter under reply, your client neither explicitly specifies the precise legal basis, the identity of the recipients or the jurisdictions that your client sends our client's personal data to.

We respond to your letter as follows:

1. Your client has not identified any specific legal basis for the transfer of our client's data in your letter. As our client has explicitly requested your client to identify the legal basis and it has only identified (I.) Article 49(1)(b) GDPR and (II.) the SCCs, we assume that they are the only legal bases that your client relies on. In accordance with Article 13 (1)(c) and Article 14 (1)(c) of GDPR please let us know if your client relies on any other legal basis and identify the explicit paragraph in the GDPR and/or the relevant other document.

2. In accordance with Article 13 (1)(c) and Article 14 (1)(c) of GDPR, please provide details of the exact processing operations, which our client's data is subject to, that are "necessary" to provide the service globally. Our client fails to see how the processing and storage of all his data in the United States is necessary for most of Facebook Ireland Limited's processing activities.

   To ensure that we fully understand your position in concrete cases, please explain how it would be for example "necessary" to permanently store data with Facebook Inc. when:

   a) Messages are sent between our client and his approximately 400 non-US friends
   b) Pictures, videos and other postings are uploaded and stored on facebook.com, beyond the potential necessity of US friends to individually load such content that is stored in the EU/EEA.
   c) Events are created by our client, but no US users are invited
   d) Facebook collects tracking data about our client on third party pages
   e) Facebook uses our client's data for research purposes
   f) Facebook generates lists of potential interest of our client

In the absence of any clear explanation, our client will assume that the transfer of our client's data in such cases is in no way "necessary" for any alleged contract.

3. The text that you quoted from your client's Data Policy in paragraph 1 of your letter under reply in essence describes that our client's data may be transferred to *any* country in the world and to *any* other controller or processor without limitation. This clearly constitutes a breach of GDPR. Please provide the details of the exact recipients of our client's data, the exact jurisdictions our client's data is sent to and furnish us with a copy of any contract or agreement relied on in the transfer our client's data to these recipients - including possible sub-contracting agreements foreseen by the SCCs.

   In the absence of any clear response, our client will assume that your client only outsourced our client's data to Facebook Inc., who in turn do not use further sub-processors.

4. The document that you provided purporting to be an extract from the SCC between your client and Facebook Inc. is unfortunately not sufficient to comply with your client's obligations under the relevant Clause of the SCCs and Article 13(1)(f), 14(1)(f) and 15(1)(c) and (2) of GDPR.

   It is an unsigned and undated raw text that departs from a copy SCC that you have provided to our client some years ago. Please provide a dated and signed copy of the current SCCs and/or any other agreement or supplementary agreement your client may use, as you have done before. In the absence of such documentation, our client will assume that your client does currently not have legally binding SCCs in place.

5. As you are aware, in accordance with the findings by the CJEU in C-311/18 Schrems, a data exporter and data importer in relying on SCC's as a basis for transferring data, are required to verify, prior to any transfer, that the level of protection required by EU law is respected in the third country (para 142 of C-311/18 Schrems). Further it is clear from paragraphs 150 to 202 of C-311/18 Schrems that the level of protection required by EU law is not present in the United States due to, *inter alia*, 50 USC § 1881a and EO 12.333. Your client has stated publicly, that Facebook Inc. has provided access to more than 100,000 accounts under 50 USC § 1881a in the first half of 2019 alone (see for example https://transparency.facebook.com/government-data-requests/country/US).

   Please provide details of the factual and legal reasoning that your client and Facebook Inc. rely upon to verify that our client's data is (contrary to this public statement) not subject to 50 USC § 1881a and EO 12.333 and/or the measures undertaken to ensure that our client's data is protected to the level required by EU law despite being subject to these laws. In absence of any such proof, our client will assume that your client is relying on the SCCs in breach of the CJEU's judgment in C-311/18 Schrems.

In circumstances where the above information and documentation should have been included in your original response and is readily accessible by your client, on behalf of our client, we request that your client reply by close of business Tuesday, 25 August 2020.

We look forward to hearing from you.

Yours faithfully,

Ahern Rudden Quigley

Ahern Rudden Quigley

Email: [redacted]

MASON
HAYES &
CURRAN

Barrow Street
Dublin 4, Ireland
D04 TR29
DX11 Dublin
+353 1 614 5000
dublin@mhc.ie

Ahern Rudden Quigley
Solicitors
5 Clare Street
Dublin 2

BY E-MAIL ONLY – [redacted]

25 August 2020	**Your ref:**	GR/MC/SCH002-	**Our ref:**	CMO/AYN/37079.52 MHC-23178695-1

Matter: DPC – v- Facebook Ireland Limited & Maximillian Schrems

Our client: Facebook Ireland Limited

Your client: Maximillian Schrems

Dear Sirs

We refer to your letter dated 21 August 2020.

Our client has already provided your client with all of the information to which he is entitled under GDPR. Similarly, your correspondence does not identify any basis for the requested information in the context of the litigation, nor indeed does it identify any other reason as to why your client is entitled to more information than that which he has already been provided. Accordingly, we kindly refer you to our letter of 19 August 2020.

Yours faithfully

Sent by email, no signature

MASON HAYES & CURRAN LLP