PROCESSOR TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

If applicable, this attachment forms part of the Okta Data Processing Addendum available at https://www.okta.com/trustandcompliance/, or other agreement between Customer and Okta governing the processing of Customer Data (the "DPA"). Unless otherwise defined in this attachment, capitalized terms used in this attachment have the meanings given to them in the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each 'data importer').

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

([1]) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

[INTENTIONALLY OMITTED]

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter([2]).

([2]) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

([3]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance,

the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.([4]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely

([4]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do

([5]) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable

obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred

personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDICES

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity named as "Customer" in the DPA.

Address: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Contact person's name, position and contact details: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Signature and date: By executing the DPA, and if applicable, the data exporter will be deemed to have signed this Annex I.

Role (controller/processor): Processor

Data importer(s):

Name: Okta, Inc.

Address: 100 First Street, San Francisco, California 94105, USA

Contact person's name, position and contact details: Timothy McIntyre, Data Protection Officer, privacy@okta.com

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Signature and date: *Timothy McIntyre* (July 19, 2021)

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendor

- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of personal data transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- First and last name
- Business contact information (company, email, phone, physical business address)
- Personal contact information (email, cell phone)
- Title
- Position
- Employer
- ID data
- Professional life data
- Personal life data (in the form of security questions and answers)
- Connection data
- Localization data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter may submit special categories of data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include Personal Data concerning health information. If applicable, data exporter agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in the Trust & Compliance Documentation (as defined by this DPA) and Documentation (as defined in the Agreement), and has determined that such restrictions and safeguards are sufficient.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Subject to Customer's use of the Service, Personal Data will be transferred on a continuous basis during the term of the Agreement.

Nature of the processing

Identity and access management and related services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by the data importer is the performance of the Service pursuant to the Agreement and as instructed by data exporter in its use of the Service.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data exporter may retain Personal Data in the Service the duration of the Agreement. Personal Data within the Service post-termination of the Agreement will be retained and deleted in accordance with the Documentation.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors may only Process Personal Data as necessary for the performance of the Service pursuant to the Agreement and for the duration of the Agreement. Sub-processor information are made available on Okta's 'Agreements' webpage (accessible via www.okta.com/agreements under the "Trust & Compliance Documentation" link).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority.

okta

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Okta maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in the Trust & Compliance Documentation (accessible via https://www.okta.com/trustandcompliance/). Okta regularly monitors compliance with these safeguards. Okta will not materially decrease the overall security of the Service during a subscription term. Okta's Service is designed to permit data exporter to manage Data Subject Requests without assistance from Okta. If data exporter cannot complete its obligations pursuant to a Data Subject Request without assistance from Okta, then, and as set forth in Section 6 of the DPA, factoring into account the nature of the Processing, Okta shall assist data exporter by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of data exporter's obligation to respond to a Data Subject Request.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Okta conducts reasonable due diligence and security assessments of Sub-processors, and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in the Security & Privacy Documentation within Trust & Compliance Documentation. Okta will work directly with Sub-processors, as necessary, to provide assistance to data exporter.

okta

ANNEX III

DATA TRANSFERS FROM THE UNITED KINGDOM AND SWITZERLAND

In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), the following provisions apply:

1. General and specific references in the Standard Contractual Clauses to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable.

2. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

3. Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

4. Where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

処理者から処理者への標準契約条項

該当する場合、この添付書類は https://www.okta.com/trustandcompliance/ で入手できる Okta データ処理補遺、またはお客様および Okta の間で交わす、お客様データの処理に適用されるその他契約（「DPA」）の一部を形成する。この添付書類で特に定義されていない限り、この添付書類の英文にて使用される大文字で始まる用語は、DPA で定義される意味を有する。

第 I 章

第 1 条

目的および範囲

(a) 本標準契約条項の目的は、個人データの処理に関する自然人の保護、および個人データの第三国移転時の当該データの自由な移動に関する欧州議会の EU 規則 2016/679 および 2016 年 4 月 27 日の評議会（一般データ保護規則）([1])についての要件の遵守を確実にすることである。

(b) 当事者:

(i) 別紙 I.A に記載されている個人データを移転する、自然人または法人、官庁、政府機関、またはその他の団体（以下、「事業体」）（以下、各「データ輸出者」）、および

(ii) 別紙 I.A に記載されているとおり、本条項の当事者でもある別の事業体を介して直接的または間接的にデータ輸出者から個人データを受け取る第三国の事業体（以下、各「データ輸入者」）。

は、本標準契約条項（以下、「本条項」）に合意した。

(c) 本条項は、別紙 I.B で特定される個人データの移転に関して適用される。

(d) 参照されている別紙を含む本条項の附属書は、本条項の不可欠な一部を構成する。

第 2 条

本条項の効果および不変性

(a) 本条項は、EU 規則 2016/679 の第 46 条(1)および第 46 条(2)(c)に基づくデータ主体の強制力のある権利および有効な法的救済を含む適切な保護措置、および管理者から処理者へ

([1]) データ輸出者が EU 規則 2016/679 の対象となる処理者であり、連合の機関または団体に代わって管理者として行動する場合、EU 規則 2016/679 対象外の別の処理者（復処理者）を従事させる場合の本条項に依拠することは、連合の機関、団体、事務局および機関による個人データの処理および当該データの自由な移動に関する自然人の保護に関する欧州議会および 2018 年 10 月 23 日付けの評議会の EU 規則 2018/1725 の第 29 条 (4)の遵守も保証するものであり、EC 規則 No 45/2001 および決定 No. 1247/2002/EC (OJ L 295 of 21.11.2018, p.39)を廃止するものである。ただし、本条項および管理者および処理者の間での契約またはその他の法的行為に定めるデータ保護義務と整合性が取れている範囲内であることを条件とする。これは特に管理者および処理者が決定 2021/915 に記載された標準契約条項に依拠している場合に当てはまる。

および/または処理者から処理者へのデータ転送に関して、適切なモジュールの選択、または附属書の情報を追加または更新する場合を除き、それが変更されていない限り、EU 規則 2016/679 の第 28 条(7)に基づく標準契約条項を定めている。これは、両当事者が直接的または間接的に、本条項と矛盾しないこと、またはデータ主体の基本的な権利または自由を害さないことを条件として、より広い契約に本条項に定められた標準契約条項を含めること、および/またはそこに他の条項または追加の保護措置を追加することを妨げるものではない。

(b) 本条項は EU 規則 2016/679 によりデータ輸出者を対象とする義務に影響を及ぼすものではない。

第 3 条

第三者受益者

(a) データ主体は、次の例外を除き、本条項をデータ輸出者および/またはデータ輸入者に対し、第三者受益者として行使し、強制することができる。

(i) 第 1 条、第 2 条、第 3 条、第 6 条、第 7 条

(ii) 第 8.1 条(a)、(c) および (d)、第 8.9 条(a)、(c)、(d)、(e)、(f) および (g)

(iii) 第 9 条(a)、(c)、(d) および (e)

(iv) 第 12 条(a)、(d) および (f)

(v) 第 13 条

(vi) 第 15.1 条(c)、(d) および (e)

(vii) 第 16 条(e)

(viii) 第 18 条(a) および (b)

(b) (a)項は、EU 規則 2016/679 に基づくデータ主体の権利に影響を及ぼすものではない。

第 4 条

解釈

(a) 本条項が EU 規則 2016/679 で定義されている用語を使用している場合、それらの用語は、その規則におけるのと同じ意味を持つものとする。

(b) 本条項は EU 規則 2016/679 の規定に照らして読まれ、解釈されるものとする。

(c) 本条項は EU 規則 2016/679 で規定されている権利および義務と矛盾して解釈されてはならない。

第5条

優先順位

本条項が合意された時点またはその後に締結された、本条項および関連する両合意書の規定の間で矛盾が生じた場合、本条項が優先するものとする。

第6条

移転の説明

移転の詳細、特に、移転される個人データの種類とそれらが移転される目的は、別紙 I.B で指定されている。

第7条 - オプション

結合条項

[意図的に省略]

第 II 章 - 当事者の義務

第8条

データの保護措置

データ輸出者は、データ輸入者が適切な技術的および組織的措置の実施を通じて、本条項に基づく義務を果たすことができるかを判断するために合理的な努力を払ったことを保証する。

8.1 指示

(a) データ輸出者はデータ輸入者に、そのデータ管理者の指示の下で処理者としての役割を担うことを通知し、処理前にデータ輸出者はデータ輸入者がそれを知り得るようにするものとする。

(b) データ輸入者は、データ輸出者によってデータ輸入者に伝達された、管理者からの文書化された指示、およびデータ輸出者からの追加で文書化された指示に基づいてのみ、個人データを処理するものとする。かかる追加の指示は、管理者からの指示と矛盾しないものとする。管理者またはデータ輸出者は、契約期間中のデータ処理に関してさらに文書化された指示を与えることがある。

(c) データ輸入者はそれらの指示に従うことができない場合、データ輸出者にただちに通知するものとする。データ輸入者が管理者からの指示に従うことができない場合、データ輸出者はただちに管理者に通知するものとする。

(d) データ輸出者は、管理者およびデータ輸出者の間の欧州連合法または加盟国法に基づく契約またはその他の法的行為に定められているのと同じデータ保護義務を、データ輸入者に課していることを保証する([2])。

8.2 目的の制限

データ輸入者は、データ輸出者によってデータ輸入者に伝達された、管理者またはデータ輸出者からさらに指示がない限り、別紙 I.B に記載されている特定の移転目的のためにのみ、個人データを処理するものとする。

8.3 透明性

要求に応じて、データ輸出者は、両当事者によって記入された附属書を含む、本条項の写しを作成し、データ主体に無料で提供する。個人データを含む、企業秘密またはその他の機密情報を保護するために必要な範囲で、データ輸出者は写しを提供する前に、附属書本文の一部を墨消しすることができる。ただし、データ主体がその内容を理解できなかったり、権利を行使したりすることができないことの無いよう、意味のある要約を提供するものとする。要求に応じて、両当事者は墨消しされた情報を明らかにすることなく、可能な範囲で、データ主体に墨消しの理由を提供するものとする。

8.4 正確性

データ輸入者が受け取った個人データが不正確であるか、古くなっていることに気付いた場合、遅滞なくデータ輸出者にその旨を通知するものとする。この場合、データ輸入者はデータの修正または消去について、データ輸出者と協力するものとする。

8.5 データの処理および消去または返却の期間

データ輸入者による処理は、別紙 I.B で指定された期間にのみ行われるものとする。処理サービスの提供終了後、データ輸入者は、データ輸出者の選択により、管理者に代わって処理されたすべての個人データを削除して、データ輸出者にその旨を証明するか、データ輸出者に代わって処理されたすべての個人データを返却し、既存の複製を削除する。データが削除または返還されるまで、データ輸入者は、引き続き本条項の遵守を確保するものとする。データ輸入者に適用される現地の法令が、個人データの返却または削除を禁止する場合、データ輸入者は、本条項の遵守を引き続き確保することを保証し、その現地の法令の下で必要な範囲で、必要な期間だけ処理する。これは第 14 条、特に第 14 条(e)に基づいて契約期間中、第 14 条(a)の要件に合致しない法令または慣行の対象である、または対象となったと信じる理由がある場合に、データ輸出者に通知するというデータ輸入者の要件に影響を及ぼすものではない。

8.6 処理のセキュリティ

(a) データ輸入者および、送信中はデータ輸出者も、偶発的または違法な破壊、損失、改ざん、不正な開示、またはそのデータへのアクセスにつながるセキュリティ侵害（以下、「個人データ侵害」）に対する保護を含む、データのセキュリティを確保するために、適切な技術的および組織的措置を講じるものとする。適切な水準のセキュリティを評価する際に、両当事者は、最新技術、実施コスト、処理の性質、範囲、状況、目的、およびデータ主体にとっての

([2]) EU 規則 2016/679 の第 28 条(4)を参照。また、管理者が EU の機関または組織である場合は、EU 規則 2018/1725 の第 29 条(4)を参照。

処理におけるリスクを十分に考慮するものとする。両当事者は、そのようにして処理の目的を達成できる場合、送信中を含めて、特に暗号化または仮名化によることを検討するものとする。仮名化の場合、個人データを特定のデータ主体に帰属させる追加情報は、可能な場合、データ輸出者または管理者の排他的な管理下にとどめるものとする。本項に基づく義務を遵守するにあたり、データ輸入者は、少なくとも別紙 II で指定された、技術的および組織的措置を講じるものとする。データ輸入者は定期的な確認を実施して、これらの措置が、適切な水準のセキュリティを提供し続けていることを確保するものとする。

(b) データ輸入者は、契約の実施、管理、監視に厳密に必要な範囲でのみ、その人員にデータへのアクセスを許可するものとする。データ輸入者は、個人データを処理する権限を与えられた人が、守秘義務を約したか、適切な法定の守秘義務が課せられていることを確約するものとする。

(c) 本条項に基づきデータ輸入者によって処理された個人データに関し、個人データ侵害が発生した場合、データ輸入者は、その悪影響を軽減するための措置を含む、侵害に対処するために適切な措置を講じるものとする。違反に気付いたデータ輸入者はまた、不当な遅延なくデータ輸出者、および適切かつ実行可能な場合は管理者に通知するものとする。かかる通知には、より多くの情報を得ることができる連絡先、侵害の性質の説明（可能な場合は、関連するデータ主体および個人データ記録の種類および概数を含む）、その引き起こし得る結果と、起こり得る悪影響を軽減するための措置を含む、データ侵害に対処するために取られた、または提案された措置の詳細を記載するものとする。すべての情報を同時に提供することが可能ではない場合、最初の通知には、その時点で入手可能な情報を含めるものとし、さらに詳しい情報は、入手できた時点で、遅滞なく提供するものとする。

(d) データ輸入者は、データ輸出者が EU 規則 2016/679 に基づく義務を遵守できるようにするため、データ輸出者に協力し、支援するものとする。特に、処理の性質およびデータ輸入者が入手可能な情報を考慮に入れ、その管理者に通知し、それにより管理者が管轄の監督当局および影響を受けるデータ主体に通知できるようにする。

8.7 センシティブデータ

移転に人種的または民族的起源、政治的意見、宗教的または哲学的信念、または労働組合の加入状況、遺伝子データ、または自然人を一意に識別する目的での生体認証データ、健康状態または人の性生活または性的指向に関するデータ、または前科および犯罪歴に関連するデータ（以下「センシティブデータ」）を明らかにする個人データが含まれる場合、データ輸入者は、別紙 I.B に記載されている具体的な制限および/または追加の保護手段を適用するものとする。

8.8 転送

データ輸入者は、データ輸出者によってデータ輸入者に伝達された、管理者からの文書化された指示によってのみ個人データを第三者に開示するものとする。加えて、第三者が本条項の適切なモジュールに拘束されている、または拘束されることに同意する場合または以下の場合にのみ、デー

タを欧州連合([3])外の第三者（データ輸入者と同じ国または別の第三国、以下「転送」）に開示することができる。

(i) 転送が、転送を規定するEU規則2016/679の第45条に基づく十分性認定による恩恵を受けている国への転送である。

(ii) それ以外の場合、第三者はEU規則2016/679第46条または第47条に従って適切な保護手段を確保している。

(iii) 特定の行政、規制、または司法手続きにおける法的請求の確立、行使、または防御のために、転送が必要である、または

(iv) データ主体または他の自然人に関するデータの重要な利益を保護するために転送が必要である。

すべての転送は、特に目的の制限など、データ輸入者による本条項に基づくその他すべての保護手段の遵守対象となる。

8.9 文書化および遵守

(a) データ輸入者は、本条項の下での処理に関連するデータ輸出者または管理者からの問い合わせに、迅速かつ適切に対応するものする。

(b) 両当事者は、本条項の遵守を示すことができるものとする。特にデータ輸入者は、管理者のために実行される処理活動に関し、適切な記録を保持するものとする。

(c) データ輸入者は、本条項に定められた義務の遵守を示すために必要なすべての情報をデータ輸出者が利用できるようにし、データ輸出者がそれを管理者に提供するものとする。

(d) 合理的な間隔で、または違反の兆候がある場合、データ輸入者は本条項の対象となる処理活動のデータ輸出者による監査を許可し、および貢献するものとする。管理者の指示により、データ輸出者が監査を要求する場合も同様とする。監査を決定する際に、データ輸出者は、データ輸入者が保持する関連する認証を考慮に入れることができる。

(e) 管理者の指示に基づいて監査が実施される場合、データ輸出者は結果を管理者が入手できるようにしておくものとする。

(f) データ輸出者は、監査を自ら実施するか、または独立した監査人を任命するかを選択できる。監査には、データ輸入者の事業所または物理的施設での検査が含まれることがあり、適切な場合、合理的な通知をもって実施されるものとする。

(g) 両当事者は、(b)項および(c)項で言及されている監査の結果を含めた情報を、要求に応じて管轄の監督当局に提供するものとする。

([3]) 欧州経済領域に関する協定（EEA 協定）は、欧州連合内市場をアイスランド、リヒテンシュタイン、ノルウェーの3つのEEA諸国に拡大することを規定している。EU規則2016/679を含むEUのデータ保護法は、EEA 協定の対象であり、その別紙 XI に組み込まれている。従って、データ輸出者によるEEA内に所在する第三者への開示は、本条項の目的において転送に当たらない。

第9条

復処理者の利用

(a) データ輸入者は、合意されたリストから復処理者を従事させることについて、管理者から一般的な許可を得ている。データ輸入者は、復処理者を追加または替える少なくとも 10 営業日前までに、そのリストの変更の意図を管理者に書面で具体的に通知するものとする。それにより管理者に、復処理者が従事する前にかかる変更に異議を唱えるのに十分な時間を与えることとなる。データ輸入者は、管理者が異議を唱える権利を行使できるようにするために必要な情報を管理者に提供するものとする。データ輸入者は、データ輸出者に復処理者の利用を通知するものとする。

(b) データ輸入者が特定の処理活動の実行を(管理者のために)復処理者に従事させる場合、データ主体の第三者受益者の権利を含む、本条項の下でデータ輸入者を拘束するものと実質的に同等のデータ保護義務を規定する書面による契約によるものとする。([4])両当事者は、本条項を遵守することにより、データ輸入者は第 8.8 項に基づく義務を果たしたこととなることに同意する。データ輸入者は、復処理者が、本条項に基づくデータ輸入者の義務を遵守することを確保するものとする。

(c) データ輸入者は、データ輸出者または管理者の要求に応じて、かかる復処理者契約の写し、およびその後の修正契約を提供するものとする。企業秘密またはその他、個人データを含む機密情報を保護するために必要な範囲で、データ輸入者は写しを提供する前に、契約書の文面を墨消しすることができる。

(d) データ輸入者はデータ輸出者に対し、データ輸入者との契約に基づく復処理者の義務の履行について、すべての責任を負うものとする。データ輸入者は、復処理者がその契約に基づく義務の履行を怠ったとき、データ輸出者に通知するものとする。

(e) データ輸入者は、復処理者と第三者受益者条項に合意するものとし、それにより、データ輸入者が事実上消滅した、法律上存在しなくなった、または支払不能となった場合に、データ輸出者は、復処理者契約を解約し、個人データを消去または返却するよう復処理者に指示する権利を有する。

第10条

データ主体の権利

(a) データ輸入者は、データ主体から受け取った要求について、管理者から承認されていない限り、その要求に対応することなく、データ輸出者と、必要に応じて管理者に速やかに通知するものとする。

(b) データ輸入者は必要に応じて、適切な場合はデータ輸出者と協力し、管理者が EU 規則 2016/679 または EU 規則 2018/1725 に基づく該当するデータ主体の権利の行使に係る要求に対応する義務を果たす支援をするものとする。この点に関して、両当事者は、提供される

([4]) 本要件は、第 7 条に従い、復処理者が適切なモジュールの下で本条項に同意することによって満たされることもできる。

支援の処理の性質および必要な支援の範囲と程度を考慮した適切な技術的および組織的措置を別紙 II に記載するものとする。

(c) (a)項および(b)項に基づく義務を履行するにあたり、データ輸入者は、データ輸出者によって伝達された、管理者からの指示に従うものとする。

第 11 条

救済

(a) データ輸入者は、データ主体に対して、個別の通知またはそのウェブサイト上に、透明かつ簡単にアクセスできる形式で苦情を処理する権限を有する連絡先を通知するものとする。また、データ主体から受け取った苦情に速やかに対処するものとする。

(b) 本条項への遵守に関して、データ主体といずれかの当事者との間で紛争が発生した場合、その当事者は、問題を友好的かつ適時に解決するために最善の努力を尽くすものとする。両当事者は、かかる紛争についてお互いに情報を提供し続けるものとし、適切な場合、その解決に協力する。

(c) 第 3 条に従って、データ主体が第三者受益者の権利を行使する場合、データ輸入者は、以下のデータ主体の決定を受け入れるものとする。

(i) 加盟国の常居所または職場の監督当局、または第 13 条に基づく管轄の監督当局に苦情を申立てること。

(ii) 紛争を第 18 条で定める管轄裁判所に提起する。

(d) 両当事者は、EU 規則 2016/679 の第 80 条(1)に定められた条件の下で、データ主体が非営利団体、組織、または団体によって代表される可能性があることを認める。

(e) データ輸入者は、該当する EU または加盟国の法律に基づいて拘束力を持つ決定に従うものとする。

(f) データ輸入者は、データ主体の選択が、適用法に従って救済を求めるための、その実体上および手続上の権利を損なうことはないことに同意する。

第 12 条

責任

(a) 各当事者は、本条項の違反に起因して他方当事者に生じた損害について、他方当事者に対して責任を負うものとする。

(b) データ輸入者またはその復処理者が本条項に基づく第三者受益者の権利を侵害することによってデータ主体に引き起こした重大または重大ではない損害について、データ輸入者はデータ主体に責任を負うものであり、データ主体は賠償を受ける権利を有するものとする。

(c) (b)項の定めにかかわらず、データ輸出者またはデータ輸入者（またはその復処理者）が、本条項に基づく第三者受益者の権利を侵害することにより、データ主体に引き起こした重大ま

たは重大ではない損害について、データ輸出者はデータ主体に対して責任を負うものとし、そしてデータ主体は、賠償を受ける権利を有するものとする。これは、データ輸出者の責任およびデータ輸出者が管理者に代わる処理者である場合、EU 規則 2016/679 または EU 規則 2018/1725 が適用されるデータ輸出者の責任に影響を及ぼすものではない。

(d) データ輸出者が(c)項に基づきデータ輸入者（またはその復処理者）に起因した損害について責任を負う場合、データ輸出者は、損害に対するデータ輸入者の責任に対応する部分の賠償金を、データ輸入者から返金を請求する権利を有することに両当事者は同意する。

(e) 本条項への違反の結果として、複数の当事者がデータ主体に生じた損害について責任を負う場合、責任を負うすべての当事者は連帯責任を負い、データ主体はこれらいずれの当事者に対しても訴訟を起こす権利を有する。

(f) 両当事者は、一方当事者が(e)項に基づいて責任を負う場合、他当事者の損害に対する責任に対応する部分の賠償金を請求する権利を有するものとする。

(g) データ輸入者は、自身の責任を回避するために復処理者の行為を理由とすることはできない。

第 13 条

監督

(a) データ輸出者が EU 加盟国内で設立されている場合: 別紙 I.C に示されているようにデータ移転に関して、データ輸出者による EU 規則 2016/679 の遵守を確保する責任を負っている監督当局が、管轄の監督当局としての役割を担うものとする。

データ輸出者が EU 加盟国で設立されていないが、EU 規則 2016/679 の第 3 条(2)に従って地域的適用範囲に含まれる場合で、EU 規則 2016/679 の第 27 条(1)に従って代表者を任命している場合: 別紙 I.C に示されているように、EU 規則 2016/679 の第 27 条(1)の意味において代表者が設立された、加盟国の監督当局が、管轄の監督当局としての役割を担うものとする。

データ輸出者が EU 加盟国で設立されていないが、EU 規則 2016/679 の第 3 条(2)に従って地域的適用範囲に含まれる場合で、ただし EU 規則 2016/679 の第 27 条(2)に従って代表者を任命していない場合: 別紙 I.C に示されているように、データ主体に対する商品もしくはサービスの提供に関連してその個人データが本条項に基づいて移転される、またはその行動が監視されている、データ主体が所在する加盟国の監督当局が、管轄の監督当局としての役割を担うものとする。

(b) データ輸入者は、本条項への遵守を確実にすることを目的として、管轄権を有する監督当局の管轄に服し、いかなる手続についても管轄の監督当局に協力することに同意する。特にデータ輸入者は、問い合わせに応答し、監査を受け入れ、監督当局によって採用された是正措置と賠償措置を含む措置を遵守することに同意する。必要な措置が講じられたことを、監督当局に書面による確認を提出するものとする。

第 III 章 – 公的機関によるアクセスの場合の現地法令および義務

第 14 条

本条項の遵守に影響を与える現地の法令および慣行

(a) 両当事者は、データ輸入者による個人データの処理に適用される、個人データを開示するための要件または公的機関によるアクセスを許可する措置を含むデータ移転先の第三国の法令および慣行が、データ輸入者が本条項に基づく義務を履行することを妨げるものであることを信じる理由がないことを保証する。これは、基本的権利および自由の本質を尊重する法令および慣行が、EU 規則 2016/679 の第 23 条(1)に記載されている目的の 1 つを保護するための民主主義社会で必要かつ比例したものを超えず、本条項と矛盾していないという理解に基づくものである。

(b) 両当事者は、(a)を保証するにあたり、特に以下の要素を十分に考慮していることを宣言する。

(i) 処理チェーンの長さ、関与する人数および使用される伝送チャネル、意図される転送、受領者の種類、処理の目的、移転された個人データの種類および形式、移転が発生する経済分野、移転されたデータの保存場所を含む、移転の具体的な状況。

(ii) 公的機関へのデータの開示を必要とする、またはかかる機関によるアクセスを許可するものを含む、移転の具体的な状況および適用される制限および保護措置([5])に関連する、移転先の第三国の法令および慣行。

(iii) 送信中および移転先国での個人データの処理に適用される対策を含む、本条項に基づく保護措置を補足するために講じられている、関連する契約上、技術上、または組織上の保護措置。

(c) (b)項に基づく評価を実施するにあたり、データ輸入者は、データ輸出者に関連情報を提供するために最善を尽くし、本条項の遵守を確保するために、データ輸出者との協力を継続することを保証する。

([5]) 本条項の遵守に対するかかる法令および慣行の影響に関して、全体的な評価の一部として、さまざま要素を考慮することができる。かかる要素には、十分に代表的な期間における、公的機関からの開示要求の以前の事例、またはかかる要求がなかったことに関連する文書化された実務経験を含めることができる。これは、特にデューデリジェンスおよび上級管理職レベルで認証された、継続的に作成された内部記録またはその他の文書を指し、ただし、第三者と適法に共有することができる情報であることを条件とする。この実践的な経験が、データ輸入者により本条項を遵守することを妨げることはないことを結論づけるために依拠される場合、他の関連する客観的な要素によって裏付けられる必要があり、両当事者は、これらの要素を合わせて、その信頼性と代表性の観点から、この結論を支持するために十分な重みを持っているか否かを、慎重に検討するものとする。特に両当事者は、同じ分野内の要求の有無および/または判例法や独立した監督機関による報告など、実際の法律の適用について、公的に入手可能な、またはその他の方法でアクセス可能な、信頼できる情報により、その実践的な経験が裏付けられており矛盾しないことを考慮に入れる必要がある。

(d) 両当事者は、(b)項に基づく評価を文書化し、要求に応じて、管轄の監督当局に提供することに同意する。

(e) データ輸入者は、本条項に同意した後および契約期間中、(a)項の要件と一致しない、法令または慣行の適用を受けることになったと信じる理由がある場合、データ輸出者に速やかに通知することに同意する。これには、第三国の法令または措置の変更または(開示要求などの)措置に従うことを含む、(a)項の要件に沿っていない法令または慣行の適用が含まれる。データ輸出者は、通知を管理者に転送するものとする。

(f) (e)項に基づく通知後、またはデータ輸出者が他の理由により、データ輸入者が、本条項に基づく義務を履行することができないと信じる理由がある場合、データ輸出者は適切な場合、管理者と相談の上、状況に対処するためにデータ輸出者および/またはデータ輸入者によって取られるべき、(セキュリティおよび機密性を確保するための技術的または組織的な対策などの)適切な措置を速やかに特定するものとする。データ輸出者は移転のための適切な保護手段が確保できないと考える場合、または、管理者もしくは管轄の監督当局からそのように指示された場合、データ移転を停止するものとする。この場合、データ輸出者は、本条項の基づく個人データの処理に関する限りにおいて、契約を解約する権利を有するものとする。契約に 2 を超える当事者が含まれる場合、データ輸出者は、全当事者が別段の合意をしない限り、関係する当事者に関してのみ、この解約権を行使することができる。本条項に基づいて契約が解約された場合は、第 16 条 (d) および (e) が適用されるものとする。

第 15 条

公的機関によるアクセスの場合のデータ輸入者の義務

15.1 通知

(a) データ輸入者は次の場合、データ輸出者および、可能な場合には、(必要に応じてデータ輸出者の支援を得て)速やかにデータ主体に通知することに同意する。

(i) 本条項に基づいて移転された個人データの開示に関する移転先国の法令に基づき、司法当局を含む公的機関から法的拘束力のある要求を受け取った場合。かかる通知には、要求された個人データ、要求している機関、要求の法的根拠および提供された回答に関する情報を含めるものとする、または

(ii) 本条項に基づいて移転された個人データに対する、移転先国の法令に従い公的機関による直接アクセスに気付いた場合。かかる通知には、輸入者が入手できるすべての情報を含めるものとする。

データ輸出者は、通知を管理者に転送するものとする。

(b) 移転先国の法令の下で、データ輸入者がデータ輸出者および/またはデータ主体に通知することを禁止されている場合、データ輸入者は可能な限り多くの情報を可能な限り早く伝達する目的で、禁止の免除を得るために最善の努力を尽くすことに同意する。データ輸入者は、データ輸出者の要求に応じて示すことができるようにするため、尽くした最善の努力を文書化することに同意する。

(c) 移転先国の法令で許可されている場合、データ輸入者は、データ輸出者に契約期間中、定期的に、受け取った要求について可能な限り多くの関連情報（特に、要求の回数、要求されたデータの種類、要求している機関、要求に異議が唱えられたか否か、およびかかる異議の結果など）を提供することに同意する。データ輸出者は、情報を管理者に転送するものとする。

(d) データ輸入者は契約期間中、(a)項から(c)項に基づく情報を保存すること、および要求に応じて管轄の監督当局に提供することに同意する。

(e) (a)項から(c)項は、第 14 条(e)および第 16 条に基づくこれらの条項を遵守できない場合にデータ輸出者に速やかに通知するデータ輸入者の義務影響を及ぼすものではない。

15.2 合法性およびデータ最小化の検討

(a) データ輸入者は、開示要求の合法性を検討すること、特に、開示を要求している公的機関に与えられた権限の範囲内にあるか否か、開示要求の合法性を慎重に評価した後、その要求が移転先国の法令、国際法および国際礼譲の原則に基づき適用される義務の下で違法であると考える合理的な理由があると結論付けた場合、要求に異議を申立てることに同意する。データ輸入者は前記と同じ条件の下で、訴えの可能性を追求するものとする。要求に異議を申立てる場合、データ輸入者は、管轄の司法当局が本案を決定するまで、要求の効力を停止する目的で、暫定措置を求めるものとする。適用される手続上の規則に基づき、義務付けられるまで、要求された個人データを開示してはならない。これらの要件は、第 14 条(e)に基づくデータ輸入者の義務に影響を及ぼすものではない。

(b) データ輸入者は、その法的評価および開示の要求に対する異議申立てを文書化すること、および移転先国の法令の下で許容される範囲で、データ輸出者がその文書を利用できるようにすることに同意する。また、要求に応じて管轄の監督当局が利用できるようにするものとする。データ輸出者は、評価を管理者が利用できるようにするものとする。

(c) データ輸入者は、開示要求に応じる場合、要求に対する合理的な解釈に基づき、許容される最小限の情報を提供することに同意する。

第 IV 条 – 最終規定

第 16 条

本条項の違反および解約

(a) データ輸入者は、いかなる理由においても本条項を遵守できない場合、データ輸出者に速やかに通知するものとする。

(b) データ輸入者が本条項に違反している場合、または本条項を遵守できない場合、データ輸出者は、遵守が再び確保されるか、契約が解約されるまで、データ輸入者への個人データの移転を一時停止するものとする。これは、第 14 条(f)に影響を及ぼすものではない。

(c) データ輸出者は以下の場合、本条項に基づく個人データの処理に関する限り、契約を解約する権利を有するものとする。

(i) データ輸出者が (b)項に従ってデータ輸入者への個人データの移転を一時停止し、合理的な期間内、およびいかなる場合も一時停止から 1 か月以内に、本条項の遵守が回復されない場合。

(ii) データ輸入者が本条項に重大もしくは持続的な違反をしている場合、または

(iii) データ輸入者が本条項に基づく義務に関して、管轄裁判所または管轄監督当局の拘束力のある決定に従わない場合。

これらの場合、かかる違反について管轄監督当局および管理者に通知するものとする。契約に 2 を超える当事者が含まれる場合、データ輸出者は、全当事者が別段の合意をしない限り、関係する当事者に関してのみ、この解約権を行使することができる。

(d) (c)項に従って契約の解約前に移転された個人データは、データ輸出者の選択において、直ちにデータ輸出者に返還されるか、そのすべてが削除されるものとする。すべてのデータの複製についても同様とする。データ輸入者は、データの削除をデータ輸出者に証明するものとする。データが削除または返還されるまで、データ輸入者は、引き続き本条項の遵守を継続して確保するものとする。データ輸入者に適用される現地法令が、移転された個人データの返還または削除を禁止する場合、データ輸入者は、本条項の遵守を引き続き確保することを保証し、その現地法の下で要求される範囲で、必要な期間においてのみデータを処理する。

(e) いずれの当事者も、以下いずれかの場合、本条項に拘束されるという合意を取り消すことができる。(i) 本条項が適用される個人データの移転を対象とする EU 規則 2016/679 の第 45 条(3)に従って欧州委員会が決定を採択した場合、または (ii) EU 規則 2016/679 が、個人データの移転先となる国の法的枠組みの一部となった場合。これは、EU 規則 2016/679 に基づく問題の処理に適用される他の義務に影響を及ぼすものではない。

第 17 条

準拠法

本条項は、その法律が第三者受益者の権利を認めている場合に限り、いずれかの EU 加盟国の法律に準拠するものとする。両当事者は、それがフランス法であることに合意する。

第 18 条

裁判所および管轄の選択

(a) 本条項から生じるすべての紛争は、EU 加盟国の裁判所において解決されるものとする。

(b) 両当事者は、それをフランスの裁判所とすることに同意する。

(c) データ主体は、その常居所とする加盟国の裁判所に、データ輸出者および/またはデータ輸入者に対して訴訟を提起することができる。

(d) 両当事者は、かかる裁判所の管轄に服することに同意する。

附属書

別紙 I

A.　当事者の一覧

データ輸出者:

氏名: DPA で「お客様」とされる法人。

住所:　Okta アカウントに関連付けられている、または DPA もしくは本契約で特定されているお客様の所在地。

連絡先担当者の氏名、役職、連絡先の詳細: Okta アカウントに関連付けられている、または DPA または本契約で特定されているお客様の所在地。

本条項の下で移転されたデータに関連する活動: 本契約およびデータ処理補遺の条件に従って、データ輸出者の指示によりアイデンティティおよびアクセス管理クラウドサービスを実行するためのお客様データである個人データの処理。

署名および日付: DPA を締結することにより、適用される場合、データ輸出者は本別紙 I に署名したものとみなされる。

役割(管理者/処理者): 処理者

データ輸入者:

名称: Okta, Inc.

住所: 100 First Street, San Francisco, California 94105, USA

連絡先担当者の氏名、役職、連絡先の詳細: Timothy McIntyre、データ保護責任者、privacy@okta.com

本条項の下で移転されたデータに関連する活動: 本契約およびデータ処理補遺の条件に従って、データ輸出者の指示によりアイデンティティおよびアクセス管理クラウドサービスを実行するためのお客様データである個人データの処理。

署名および日付: Timothy McIntyre (2021 年 7 月 19 日)

役割(管理者/処理者): 処理者

B.　**移転の説明**

個人データが移転されるデータ主体の種類

データ輸出者は、データ輸出者が独自の裁量で決定および支配する範囲で、本サービスに個人データを送信することができる。これには、以下のデータ主体の種類に関連する個人データが含まれるがこれらに限定されない。

- データ輸出者のお客様、ビジネスパートナー、ベンダー（いずれも自然人）
- データ輸出者のお客様、ビジネスパートナー、ベンダーの従業員または連絡担当者
- データ輸出者がサービスの使用を許可したすべての従業員、代理人、顧問、請負人、またはユーザー（いずれも自然人）

移転される個人データの種類

データ輸出者は、データ輸出者が独自の裁量で決定および支配する範囲で、本サービスに個人データを送信することができる。これには、以下の個人データの種類が含まれるがこれらに限定されない。

- 氏名
- ビジネス用の連絡先情報（会社名、電子メール、電話、会社の物理的住所）
- 個人用の連絡先情報（電子メール、携帯電話）
- 役職
- 職位
- 雇用者
- ID データ
- 職歴データ
- 個人的な生活データ（セキュリティの質問および回答の形式）
- 接続データ
- 位置データ

移転されるセンシティブデータ（該当する場合）および適用される制限または保護措置で、例えば厳密な目的の制限、アクセスの制限（専門的なトレーニングを受けたスタッフのみのアクセスを含む）など、データの性質およびそれに伴うリスクを十分に考慮し、データへのアクセス、転送の制限、または追加のセキュリティ対策の記録の保持。

データ輸出者は、データ輸出者が独自の裁量で決定および支配する範囲で、健康に関する個人データを含むことがある特別な種類のデータを本サービスに送信することがある。該当する場合、データ輸出者は、「Trust & Compliance Documentation（信頼とコンプライアンスに関する文書）」（この DPA で定義される）および関連文書（本契約で定義される）に記載されている措置を含む、特別な種類の個人データに適用される制限および保護措置を確認および評価し、かかる制限および保護手段が十分であると判断したことに同意する。

移転の頻度（例えば、データの移転が 1 回限りか、継続的に行われるか）

お客様による本サービスの利用に基づき、個人データは、本契約の期間中、継続的に移転される。

処理の性質

本契約に基づくアイデンティティおよびアクセス管理および関連サービス。

データ移転およびさらなる処理の目的

データ輸入者による個人データ処理の目的は、本契約に基づく、および本サービスの利用においてデータ輸出者から指示されたとおりの、本サービスの実行である。

個人データが保持される期間、またはそれが可能ではない場合は、その期間を決定するために使用される基準

データ輸出者は、本契約の期間中、本サービス内で個人データを保持することがある。本契約終了後の本サービス内の個人データは、関連文書に従って保持および削除される。

(復)処理者への移転の場合、処理の主題、性質、期間も指定

復処理者は、本契約に従いおよび本契約期間中、本サービスの実行に必要な範囲においてのみ個人データを処理できる。復処理者の情報は、Okta の「Agreements」ウェブページ(www.okta.com/agreements の「Trust & Compliance Documentation」リンクからアクセス可能)で入手できる。

C. 管轄の監督当局

第 13 条に基づき管轄の監督当局を特定

データ輸出者が EU 加盟国内で設立されている場合: 監督当局はデータ移転に関して、データ輸出者による EU 規則 2016/679 の遵守を確保する責任を負う監督当局が、管轄の監督当局としての役割を担うものとする。

データ輸出者が EU 加盟国内で設立されていないが、EU 規則 2016/679 の第 3 条(2)に従って地理的適用範囲に含まれる場合、かつ EU 規則 2016/679 の第 27 条(1)に従って代表者を任命している場合: EU 規則 2016/679 の第 27 条(1)の意味における代表者が設立された、加盟国の監督当局が、管轄の監督当局としての役割を担うものとする。

データ輸出者が EU 加盟国内で設立されていない場合、ただし EU 規則 2016/679 の第 3 条(2)に従って地理的適用範囲に含まれる場合で、EU 規則 2016/679 の第 27 条(2)に従って代表者を任命する必要がない場合: そのデータ主体への商品またはサービスの提供に関連して、本条項の下で個人データが移転される、またはその行動が監視されている、データ主体が所在する加盟国の監督当局が、管轄の監督当局としての役割を担うものとする。

別紙 II

データのセキュリティを確保するための技術的および組織的措置を含む
技術的および組織的措置

処理の性質、範囲、状況、および目的、そして自然人の権利と自由に対するリスクを考慮に入れて、適切な水準のセキュリティを確保するために、データ輸入者によって実施されている(関連する認証を含む)技術的および組織的対策の説明。

Okta は、「Trust & Compliance Documentation」(https://www.okta.com/trustandcompliance/からアクセス可能)に記載されているとおり、個人データを含むお客様データのセキュリティ、機密性、完全性を保護するための、管理上、物理的、および技術的な保護手段を維持している。Okta は、これらの保護措置の遵守を定期的に監視している。Okta は、サブスクリプション期間中、本サービスの全体的なセキュリティを大幅に低下させることはない。Okta の本サービスは、データ輸出者が Okta の支援無く、データ主体の要求を管理できるように設計されている。データ輸出者が Okta の支援なしでは、データ主体の要求に従って義務を履行できない場合、DPA の第 6 条に記載されているように、処理の性質を勘案し、Okta は可能な限り、データ輸出者がデータ主体の要求に応じる義務を果たすため、適切な組織的および技術的手段によってデータ輸出者を支援するものとする。

(復)処理者への移転の場合も、管理者および処理者から復処理者への移転の場合にはデータ輸出者に対して支援を提供できるようにするため、(復)処理者が実施する具体的な技術的および組織的対策の説明。

Okta は、復処理者の合理的なデューデリジェンスとセキュリティ評価を実施し、「Trust & Compliance Documentation」内の「Security & Privacy Documentation(セキュリティとプライバシーに関する文書)」で規定されているものと同様またはそれよりも厳しい規定が含まれている契約を、復処理者と締結している。Okta は、必要に応じて復処理者と直接連携し、データ輸出者を支援する。

okta

別紙 III

英国およびスイスからのデータ移転

英国からの個人データの移転、および/またはスイスのデータ保護法および規制（「スイスのデータ保護法」）のみに準拠するスイスからの個人データ移転の場合、以下の規定が適用される。

1. GDPR、EU または加盟国法への標準契約条項における一般的および具体的な言及は、該当する場合、英国のデータ保護法および規則（「英国データ保護法」）またはスイスのデータ保護法における同様の言及と同じ意味を持つものとする。

2. スイスのデータ保護法に準拠するデータ移転に関しては、標準契約条項は、スイスのデータ保護法に基づきかかる情報が保護されている個人データと同様に、かかる法律が改正されることにより、法人に適用されなくなるまで、識別された、または識別可能な法人に関連する情報の移転にも適用される。

3. データ輸出者が英国で設立されている場合、または英国のデータ保護法および規則（UK Data Protection Laws and Regulations）の地理的適用範囲内にある場合、プライバシー監視機関（Information Commissioner's Office）が管轄の監督機関の役割を担うものとする。データ輸出者がスイスに設立されている場合、またはスイスのデータ保護法および規則の地理的適用範囲内にある場合、関連するデータ移転がスイスのデータ保護法および規則に準拠する限り、スイスの連邦データ保護情報コミッショナー（Federal Data Protection and Information Commissioner）が管轄の監督機関としての役割を担うものとする。

4. 本契約で英国が専属管轄権を有すると指定されている場合、英国が、標準契約条項から生じる全ての紛争を解決する専属管轄権を有するものとする。スイスを常居所とするデータ主体については、スイスの裁判所が紛争に関する管轄の代替場所となる。