

## STATEMENT OF WORK NO. 1

This Statement of Work ("SOW") is entered into as of 1<sup>st</sup> **February 2024** ("SOW Effective Date") by and between Genpact India Private Limited, a private limited company incorporated under the laws of India, and having its registered office at 12A (Ground Floor), Prakash Deep Building, 7, Tolstoy Marg, New Delhi-110001, India ("Genpact") and NextWealth Entrepreneurs Private Limited, a company incorporated under the Companies Act, 1956, and having its registered office at GB, Alsa Glenridge, No. 32, Langford Road, Bangalore – 560 025, India ("Service Provider") pursuant to the Master Terms and Conditions Agreement dated 23<sup>rd</sup> October 2023 and entered into between Genpact and Service Provider ("Agreement"). Any capitalized terms used but not defined herein will have the meanings set forth in the Agreement. This SOW is governed by the terms and conditions of the Agreement, including any amendments thereto, subject to any express modifications, additions or exclusions set forth in this SOW or addendums hereto. In the event of any conflict between the Agreement and this SOW, this SOW will prevail to the extent with respect to any clause expressly stated herein.

Service Provider will provide the following Services in accordance with the terms of this SOW.

### 1. REPRESENTATIVES

Genpact nominated representative for the SOW: Alexandra Dehnert, email: alexandra.dehnert@genpact.com

Service Provider nominated representative for the SOW: Raghu Krishnamurthy, email: raghu.krishnamurthy@nextwealth.com.

### 2. SOW TERM:

**Services Start Date: 26<sup>st</sup> Feb 2024 Services End Date: 23<sup>rd</sup> October 2025**

Genpact may terminate this SOW in whole or in part by written notice of not less than forty-five (45) days. In the event of ramp-down, parties shall mutually agree on the percentage of ramp-down each quarter.

### 3. DESCRIPTION OF SERVICES:

#### Scope of Work:

Indexing -CMV Process

Indexing includes:

- System is configured to capture attributes from the face of the invoice & other sources
- Agent to validate the captured attribute & correct as necessary
- Include additional fields to capture as per the design
- Identify type of invoices as per set procedures
- Initially, agent may needed to capture manually by pointing the cursor & there on system learns

---

Any additional scope shall be subject to mutual agreement.

**Service Provider's Responsibility:** Execute the work as defined in the SOW and achieve the agreed upon SLAs, provide a dashboard every week to be reviewed, create the process map, SOPs and checklists for the process. Service Provider is responsible for the recruiting, assessing, hiring,

training and management of hires. Service Provider is also primarily and exclusively responsible for maintaining compliance with local labor laws.

**Genpact's Responsibility:** Provide initial training, adequate process documents, feedback on the outcome on an agreed interval and access to systems and platforms as required to enable Service Provider to complete the work. In addition, Service Provider would like Genpact to support us with the following:

- Have a dedicated Point of Contact / Engagement Manager – who will be our go-to person.
- Genpact's resources to train the team at Service Provider or Genpact location for the processes in scope.
- Identify a Single Point of Contact to provide access to all systems and platforms required to do the job and clear guidelines on process to be followed for addition and deletion of access and sign-off before the team goes live.
- Provide virtual support for the initial three (3) weeks of go-live and ramp-up.
- Provide all available documentation on Training, Operations SOPs, Process Flows, Quality Methodology, Checklists, Reports, etc.

#### 4. LOCATION:

The Services will be delivered from our center at Mallasamudram near Salem, Tamil Nadu. Any new location or centers to be added in future will be mutually discussed between both the parties and agreed over email.

#### 5. EQUIPMENT:

Any access to Genpact systems, data or Confidential Information will be permitted only through laptops or other endpoints that have been either: (i) supplied by Genpact; or (ii) assessed and approved by Genpact's information security team. (Note that this assessment and approval process may differ from Genpact's Vendor Governance Assessment process).

#### 6. PERSONNEL:

All personnel delivering Services hereunder are employees of Service Provider.

#### 7. BUSINESS CONTINUITY/ DISASTER RECOVERY / BACKUP:

The Business Continuity Management Plan as agreed between the parties is appended to this SOW as Exhibit F.

#### 8. PROJECT SCHEDULE:

The project schedule is reflected as follows:

Wave	19-Feb	26-Feb	04-Mar	11-Mar	18-Mar	25-Mar	01-Apr	08-Apr	15-Apr	22-Apr	29-Apr	06-May
CMV		OB	KT	KT	GP	GP	GL					

OB	Onboarding
KT	Knowledge Transfer
GP	Guided Production
GL	Go-Live

This is an illustration and subject to change as per the contract sign-off date and mutually agreed transition timelines.

## 9. DAYS AND HOURS OF WORK:

The team will work five (5) days a week (Monday to Friday).

The Hours of Operation will be as follows:

- 9:00 AM to 6:00 PM IST

## 10. SERVICE FEES OR RATES:

All rates are based on a nine (9)-hour workday (8 productive hours/day plus 1-hour break) and a five (5)-day work week, Monday to Friday, excluding holidays where located.

**Fixed Price:** Service Provider's charges for the Services is as follows:

**Rs.40,000/-** rate/person/month (INR)

1. The mix of Fresher Vs Experienced considered is 65:35 (Freshers are candidates with less than one [1] year of relevant work experience).
2. All dedicated support staff will be invoiced at the same rate as mentioned above. This includes Team Leads, QC, Trainers and Operations Manager.
3. The ratios typically maintained are as follows:
  - Team Lead to Associates: 1:25
  - QA/QC to Associates: 1:15
  - Trainer to Associates: 1:75
  - Manager to Associates: 1:100
4. All applicable taxes (like GST) will be additional.
5. Billing will commence from the start of Genpact-specific knowledge transfer.
6. Pricing is fixed for the scope of work as mentioned here above. Any changes to scope or type or skills or complexities will need to be mutually discussed and the impact on cost or timelines to be agreed.
7. There will be a YOY increase for Cost-of-Living Adjustment at six percent (6%) per annum.
8. Service Provider will provide a productivity gain of three percent (3%) from end of year 2 for three (3) continuous years. This will be dependent on the actual billable headcount available at service provider.
9. Volume fluctuations up to ten percent (10%) will be managed by NextWealth. Any further increase in volumes will be managed on a best-efforts basis and the impact on Service Levels will need to be considered.
10. Invoices to be paid within forty-five (45) days from when it is raised.
11. Invoices will be raised by region for every month on or before the 7<sup>th</sup> of the following month in which the Services were provided. Any disputes have to be raised within 7 working days from the date the invoice is received by Genpact.
12. Any increase in minimum wages as per State or Central Government legislation will be discussed and agreed in terms of the applicable dates.

**Operations and People Related**

- One hundred and sixty-eight (168) hours per month has been considered per month for each FTE. Any overtime which requires people to stay back, work on holidays/weekly offs or national holidays, will be charged @ 1.5 times the daily rate as per the State Labour Law. Overtime will be undertaken with explicit approval from Genpact.
- Training related to the Genpact environment and processes will be provided by Genpact.
- Transition costs, if any, which requires the Service Provider team to travel to Genpact's locations will be charged additionally on actual or mutually agreed costs.
- In situations where a reverse transition is required or a project needs to be wound down, a thirty to sixty (30-60)-day notice period must be provided. Depending on the size of the team deployed at Service Provider and for the duration of the transition, the full amount per FTE will need to be paid, as applicable.
- If people are required to work before 7am and beyond 7:30pm, then there will be a Partial or Full Night shift allowance that will be applicable.
  - Partial Night Shift allowance – Rs. 3,500/person/month for shifts prior to 6 am and ending post 8 pm)
  - Full Night Shift allowance – Rs. 6,000/person/month for shifts between 8pm to 6 am

**Infrastructure and Technology Related.**

- Windows OS and anti-virus for all workstations. MS Office in addition for Team leads has been assumed. Any software over and above this if required will be charged additional at actual.
- Any tools developed specifically for the project; will be discussed and gain share/cost sharing will be mutually agreed.
- Bandwidth of up to 150 kbps broadband connectivity per seat has been considered. Anything additional would need to be discussed, reworked and agreed.
- Service Provider will provide an enclosed space for the initial team. This will be a smaller space with the opportunity to add seats in the course of the engagement.
- The cost includes the standard infrastructure like antivirus, end point security, Internet access, LAN, biometric access, CCTV, shared firewall and a secure space.
- UPS back up of two (2) hours and generator back-up has been taken into consideration.
- Genpact will be responsible for providing all required access to Systems and other applications that will be required to provide the Services.

**11. PAYMENT SCHEDULE:**

**FTE Based billing:** Billing will be done monthly based on mutually agreed head count for the month. Refer Clause 9 for FTE rate and other key billing-related matters.

All invoices will be paid in accordance with the terms of the Agreement.

**12. SERVICE LEVELS:**

The service levels as agreed between the parties are included under Exhibit E (Service Levels).

- 13. Replacement of Service Provider Personnel.** Service Provider will ensure the continuity of Service Provider Personnel assigned to perform the Services under this SOW. In the event that any Service Provider Personnel performing Services hereunder is found to be unacceptable to Genpact for any reason (including demonstration that he or she is not qualified to perform or has provided false information on his or her resume), Genpact shall notify Service Provider of such fact (without waiving any other rights or remedies it may have hereunder) and Service Provider shall promptly remove such personnel from performing Services under any SOW with Genpact. If requested by Genpact, Service Provider will promptly provide a replacement with similar experience as well as

suitable ability and qualifications who is acceptable to Genpact, at no additional cost to Genpact. In the event that any anticipated or actual delays in meeting Genpact's deadlines or scheduled completion dates for work being performed under this SOW are caused by the unacceptable performance of any Service Provider Personnel, Service Provider shall provide additional temporary Supplier Personnel, as requested by Genpact and at no additional cost to Genpact, in order to complete the applicable Services in a timely manner.

**14. Training.** Upon Genpact's request, Service Provider will cause Service Provider Personnel designated by Genpact to take Genpact's mandatory online trainings on Integrity, Data Privacy & Information Security, and other relevant trainings at Service Provider's own expense. Genpact will not reimburse Service Provider for the time spent by Service Provider Personnel to take such trainings. In the event any Service Provider Personnel does not take or satisfactorily complete any mandatory trainings required by Genpact prior to the performance of the Services or annually thereafter, Genpact reserves the right to, and Service Provider agrees that Genpact may, withhold payments of any invoice for the Services performed by such Service Provider Personnel until all required trainings are completed.

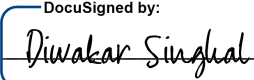
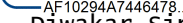
#### **15. CLIENT CONTRACT FLOWDOWNS AND OTHER TERMS**

Service Provider shall comply with all relevant Terms and Conditions of Genpact's end client contract that apply to the Services, including without limitation the terms set forth in Addendum 2 and 4 hereto. In the event of any conflict between the Agreement and the Flow Down Terms, the Flow Down Terms will prevail.

#### **15. PERSONAL DATA**

Personal Data to be processed by Service Provider in connection with the Services herein are set out in Addendum 3 - Data Protection Addendum, attached to this SOW. Service Provider acknowledges that all Personal Data are subject to the terms of the Data Privacy Provisions that is attached to the Agreement.

**IN WITNESS WHEREOF** the undersigned authorized representative of each party has executed this SOW as of the SOW Effective Date.

<p><b>Genpact (as defined at the top):</b></p> <p>By:  _____</p> <p>Name:  Diwakar Singhal _____</p> <p>Title: <u>Global Business Leader</u> _____</p>	<p><b>Service Provider (as defined at the top):</b></p> <p>By: NextWealth Entrepreneurs Pvt. Ltd.</p> <p>Name: Mythily Ramesh</p> <p>Title: CEO</p>
--	---

**ADDENDUM 1 TO SOW**  
**SOW Local Tax and Compliance Requirements**

**Delivery and Recipient Locations in Scope for this SOW:**

The Services will be delivered from Service Provider's centre at Mallasamudram near Salem, Tamil Nadu. Any new location or centres to be added in future will be mutually discussed between both the parties and agreed over email.

**Special Tax Provisions (if any):** [Not applicable]

**Local Country Compliance Requirements Applicable to SOW**

Income Tax Act

Goods & Service Tax

Shops & Establishments

Local labor laws

All employee related laws including PF, ESI, Gratuity, etc

Any other applicable laws

## EXHIBIT A

### DATA PROTECTION PROVISIONS

#### 1. DEFINITIONS AND INTERPRETATION

##### 1.1 In this Exhibit:

“**Clauses**” means the standard contractual clauses annexed to EU Commission Decision 914/2021/EU of 4 June 2021 (as updated/replaced from time to time) or, if applicable and legally sufficient, any equivalent issued by a corresponding regulator and/or government (including by the UK and Swiss government);

“**Controller**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**”, “**Processing**” (including the derivatives “**Processed**” and “**Process**”) and “**Processor**” have the meaning given to them in the GDPR or, to the extent the CCPA or other relevant law applies, the definitions given in the CCPA or such other law;

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq;

“**Data Protection Laws**” means any applicable law relating to the Processing of Personal Data and e-privacy including: (i) European Parliament Regulation (EU) 2016/679 (the “**GDPR**”) and equivalent legislation under UK and Swiss law; (ii) any corresponding national laws or regulations including any laws implementing the GDPR; (iii) the CCPA; and (iv) any corresponding guidance, codes or certification mechanisms of the relevant regulator or supervisory authority regarding such laws;

“**Data Protection Losses**” means all liabilities and amounts, including all: (i) costs (including legal costs), claims, demands, actions, settlements, losses and damages; (ii) regulatory fines, penalties and Data Subject compensation; and (iii) costs of rectification or restoration of Unilever Personal Data;

“**including**”, “**includes**” means “including/includes without limitation”;

“**Partner**” means NextWealth Entrepreneurs Private Limited, acting as a service provider to and conduit of data for Unilever and/or any Unilever Group Company;

“**Transfer Impact Assessment**” has the meaning provided to it at Paragraph 7.4 (*Assessment of International Data Transfers*) of this Exhibit C (*Data Protection Provisions*); and

“**Unilever Personal Data**” means Personal Data provided or made available to Supplier by (or collected or created for) Partner on behalf of Unilever or a Unilever Group Company in connection with the Agreement (including any SOW and Services provided under it), including as further identified in Annex 1 of an SOW (*Data Transfer Details*).

##### 1.2 The Clauses shall supplement this Exhibit and this SOW to the extent necessary to comply with applicable law governing the cross-border transfer of Unilever Personal Data originating in the European Economic Area (“**EEA**”), United Kingdom (“**UK**”), and/or Switzerland, as applicable. Specifically:

##### 1.2.1 the Processor-to-Processor Clauses set out in Part 3 (*EU Standard Contractual Clauses Module 3: Processor-to-Processor*) of Annex 3 (*Transfer Provisions*) shall apply to the

extent Supplier receives or has access to Unilever Personal Data where Supplier operates as a sub-Processor; and

- 1.2.2 the UK and Swiss addenda set out in Annexes 4 (*UK International Data Transfer Addendum to the EU Standard Contractual Clauses*) and 5 (*Swiss Addendum to the EU Standard Contractual Clauses*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*) shall amend the relevant module(s) of the Clauses in Annex 3 (*Transfer Provisions*), as applicable.
- 1.3 For the purposes of Annexes 3 (*Transfer Provisions*) and 4 (*UK International Data Transfer Addendum to the EU Standard Contractual Clauses*) of Appendix A (*Data Processing Annexes*) to this Exhibit F (*Data Protection Provisions*), references to the Appendix to the Clauses and any Annexes within the Appendix to the Clauses shall be deemed to be references to the applicable Data Transfer Details which form part of the relevant SOW, the template for which is set out in Annex 1 (*Template for Data Transfer Details*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*).
- 1.4 A reference to “Unilever” in this Exhibit means any Unilever Group Company that is the Controller of the Unilever Personal Data.
- 1.5 To the extent of any inconsistency, the order of precedence is: (1) the Clauses and (2) this Exhibit.
- 1.6 Reference to laws: (i) includes all corresponding subordinate legislation; and (ii) means that law as amended or re-enacted from time to time. An obligation to perform “in accordance with Data Protection Laws” (or similar) means in accordance with the corresponding Data Protection Laws in force at the time of performance.
- 1.7 Where the Processing of Unilever Personal Data is subject to the GDPR, a reference to a “legal obligation” in this Exhibit means an obligation pursuant to Union or Member State law.

## **2. PROCESSING OF UNILEVER PERSONAL DATA**

- 2.1 The parties agree and acknowledge that:
  - 2.1.1 Unilever is the Controller of the Unilever Personal Data and Partner shall have an agreement with Unilever to comply with all applicable Data Protection Laws in its capacity as a Processor;
  - 2.1.2 where the GDPR and equivalent legislation under UK and Swiss law applies, Supplier is a Sub-Processor and Partner is a Processor of the Unilever Personal Data ; and/or
  - 2.1.3 where the CCPA applies, Supplier and Partner each will act as a “Service Provider” (as such term is defined in the CCPA) in the performance of the Services.
- 2.2 Supplier shall only Process the Unilever Personal Data in accordance with the documented commercially reasonable instructions of Partner, including in relation to the transfer of Unilever Personal Data to a third country, unless it is under a legal obligation to do so and, in any such case Supplier shall notify Partner of that legal requirement prior to Processing, unless that law prohibits the disclosure of such information on important grounds of public interest.
- 2.3 Supplier shall:



- 2.3.1 comply with and Process all Unilever Personal Data in accordance with applicable Data Protection Laws in its capacity as a Processor or Service Provider (as applicable);
- 2.3.2 to the extent it is aware, immediately notify Partner in the event that any of its instructions infringe the Data Protection Laws;
- 2.3.3 using commercially reasonable endeavours, co-operate and assist Partner and, upon Partner's request, Unilever with any data protection impact assessments and consultations with, or notifications to, or responding to questions from or investigations by regulators or supervisory authorities regarding the Unilever Personal Data;
- 2.3.4 promptly (and in any event within two (2) Business Days) forward to Partner and otherwise cooperate with and assist Partner, and upon Partner's request, Unilever promptly with any Data Subject requests under Data Protection Laws and/or any other complaints or claims relating to the Processing of Unilever Personal Data;
- 2.3.5 maintain a record of all categories of Processing activities, consistent with the requirements of Data Protection Laws, promptly making the record available on request to Partner or, upon Partner's request, Unilever; and
- 2.3.6 not retain, use or disclose Unilever Personal Data for any other commercial purpose other than providing the Services to Partner for the purpose of Partner's services to Unilever, including services related to suppliers of Unilever.

## 2.4 **Supplier Personnel**

Supplier shall ensure the reliability of its personnel (which includes those of its authorised subcontractors) and that they: (i) receive adequate compliance training; (ii) will only Process Unilever Personal Data in compliance with this Exhibit; and (iii) are subject to an appropriate contractual or statutory duty of confidentiality.

## 2.5 **Deletion or Return of Unilever Personal Data**

Under this Exhibit, Supplier shall cease Processing Unilever Personal Data when it is no longer necessary to do so to provide the Services and/or within fifteen (15) Business Days (or such other reasonable time as may be agreed by the parties) of Partner's or Unilever's instruction to do so. If applicable, at Partner's option, Supplier shall securely delete or return the Unilever Personal Data, unless storage of the Unilever Personal Data is required under applicable law, and will provide a certificate of completion of such return or destruction.

## 2.6 **Representative Related Information**

The parties may, individually as separate Controllers (or pursuant to the CCPA, as separate businesses), need to Process Personal Data of each other's representatives including in order to: (a) resolve disputes relating to this Exhibit; and/or (b) comply with legal obligations. Each party shall conduct such Processing in accordance with their respective privacy policies.

## 3. **CCPA RESTRICTIONS AND OBLIGATIONS**

- 3.1 The following provisions apply to Unilever Personal Data to the extent it is subject to the CCPA:
  - 3.1.1 Supplier shall not "sell" (as such term is defined in the CCPA), disclose, release, transfer, make available or otherwise communicate any Unilever Personal Data to another business

or third party without the prior written consent of Unilever unless and to the extent that such disclosure is made to an authorised subcontractor in accordance with the terms of this Exhibit. Notwithstanding the foregoing, nothing in this Exhibit shall restrict Supplier's ability to disclose Unilever Personal Data to comply with applicable laws or as otherwise permitted by the CCPA; and

- 3.1.2 Supplier shall promptly (and in any event within two (2) Business Days) forward to Partner and otherwise cooperate with and, if applicable, assist Partner and, upon Partner's request, Unilever promptly with any request from a Data Subject relating to the Data Subject's right of access, right to knowledge, right of deletion, or right to opt out of "sale" (as such term is defined in the CCPA).

#### **4. SECURITY**

- 4.1 Supplier warrants it has implemented and shall maintain appropriate technical and organisational measures, internal controls and information security routines on Supplier Systems aimed to protect Unilever Personal Data against a Personal Data Breach. Supplier shall ensure a level of security appropriate to the risk of Processing the Unilever Personal Data. Supplier shall use commercially reasonable efforts to also cooperate and assist Partner and, upon Partner's request, Unilever with its security obligations under the Data Protection Laws.
- 4.2 Supplier shall put in place and comply with the security measures set out in this SOW and its Exhibits. Annex 1 (*Template for Data Transfer Details*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*) contains a template which shall be completed for this SOW which shall detail, amongst other things, technical and organisational measures deemed necessary to protect Unilever Personal Data. Annex 2 (*Supplementary Measures*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*) shall also apply, unless varied in this SOW.

#### **5. NOTIFICATION AND PERSONAL DATA BREACHES**

- 5.1 If Supplier becomes aware of or reasonably suspects the occurrence of a Personal Data Breach, it shall without undue delay and in any event within twenty-four (24) hours of the identification of any such Personal Data Breach:
  - 5.1.1 notify Partner, providing all relevant information, as required under Data Protection Laws, including, to the extent available:
    - (a) the nature of the Personal Data Breach including, where possible, the approximate number of affected Data Subjects and the volume and/or number of Unilever Personal Data records;
    - (b) any existing or anticipated involvement of regulatory authorities; and
    - (c) any measures taken, or that Supplier recommends, to deal with the Personal Data Breach and/or its adverse effects, and

if Supplier cannot reasonably provide all required details within such timeframe, it shall immediately inform Partner of the grounds for delay and expected timeframe (which may be phased) and provide subsequent updates;

- 5.1.2 investigate the Personal Data Breach and provide Partner with detailed related information;

- 5.1.3 take all reasonable steps itself and also provide all reasonable assistance to Partner (at Partner's reasonable cost, save where the Data Breach was caused solely by Supplier and/or any of its subcontractors), to remediate or mitigate any actual or potential damage from a Data Breach (including reasonably supporting any Partner or Unilever response plan) and to prevent re-occurrence (which may include removal of service personnel); and
- 5.1.4 as agreed with Unilever, cooperate in informing the relevant supervisory authorities or affected Data Subjects.

## **6. SUBCONTRACTORS**

- 6.1 Partner acknowledges and authorizes Supplier to engage third parties to Process the Personal Data ("Subprocessor"), which shall include (a) Supplier's affiliates or parent companies; and (b) third-party Subprocessors, including Subprocessors engaged by Iron Mountain's affiliates or parent.
- 6.2 Supplier shall make available to the Partner the current list of Subprocessors at this [web address].
- 6.3 If Supplier makes any additions or changes to the list linked in 6.2, Supplier shall notify the Partner by email in advance of such addition or replacement. In order to receive these email notifications, the Partner shall subscribe and manage any existing subscription to Supplier's notification mechanism via this [web page]. If the Partner fails to subscribe to this notification service, Supplier shall not be liable for the lack of Subprocessor notification and all such appointments shall be deemed to be authorized by the Partner. If the Partner subscribes, the appointment of any new Subprocessor shall be deemed authorized by the Partner unless Partner reasonably objects on demonstrable grounds that relate to data protection in writing and within fifteen (15) days of Supplier's provision of notice. If Partner reasonably objects on demonstrable grounds related to data protection in writing and within the given timeline, Supplier will use reasonable efforts to change the Services to avoid processing of the Personal Data by such proposed Subprocessor. If Supplier is unable to implement such changes within a reasonable period of time, then such new Subprocessor shall not Process the Partner's Personal Data and the Partner shall as promptly as possible take possession of such assets, subject to the terms of the Agreement and at the Partner's cost and expense.
- 6.4 Supplier shall impose contractual terms on its Subprocessors which are substantially similar to those set out in this Exhibit.
- 6.5 Supplier is obliged to regularly monitor the performance of its Subprocessors and it remains liable for the performance of the Personal Data processing activities under this Exhibit by its Subprocessors.

## **7. TRANSFERS OF DATA**

### **7.1 Transfers from the EU/EEA to countries outside the EU/EEA**

To the extent that Unilever Personal Data originating in the EU/EEA is transferred outside of the EU/EEA, the relevant Clauses in Annex 3 (*Transfer Provisions*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*) shall apply.

## 7.2 Transfers originating in the UK or Switzerland

To the extent that Unilever Personal Data originating in the UK or Switzerland is transferred outside of the UK or Switzerland respectively, the UK Addendum in Annex 4 (*UK International Data Transfer Addendum to the EU Standard Contractual Clauses*) of Appendix A (*Data Processing Annexes*) or the Swiss Addendum in Annex 5 (*Swiss Addendum to the EU Standard Contractual Clauses*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*), as applicable, shall apply.

## 7.3 Other transfers out of originating country

For transfers not covered by Paragraphs 7.1 (*Transfers from the EU/EEA to countries outside the EU/EEA*) or 7.2 (*Transfers originating in the UK or Switzerland*), Supplier may only transfer Unilever Personal Data outside of the originating country where any such transfer complies with applicable Data Protection Laws.

## 7.4 Assessment of International Data Transfers

Supplier shall reasonably support Partner or, upon Partner's request, Unilever when such party conducts an international data transfer impact assessment "**Transfer Impact Assessment**".

## 7.5 Transfer Risk Assessment and Supplementary Measures

Pursuant to the Clauses, Supplier shall:

- 7.4.1 assess the laws applicable to it and determine whether such laws, including laws enabling compelled disclosure or access by public authorities, prevent Supplier from complying with its obligations under the Clauses to ensure a level of protection for Personal Data that is essentially equivalent to the GDPR;
- 7.4.2 implement the supplementary measures pre-selected in Annex 2 (*Supplementary Measures*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*), or as otherwise agreed by the Parties in an SOW, as well as any additional supplementary measures that it selects or describes in Annex 2 (*Supplementary Measures*) of Appendix A (*Data Processing Annexes*) to this Exhibit C (*Data Protection Provisions*) where indicated; and
- 7.4.3 provide all information reasonably requested by Unilever for the purpose of completing the assessment required by the Clauses.

# 8. GOVERNMENT OR PUBLIC AUTHORITY REQUESTS FOR PERSONAL DATA

## 8.1 Access by Intelligence Services

Supplier warrants that Supplier and its subcontractors that have access to Unilever Personal Data: (i) are not subject to any other law that could be seen as undermining the protection of personal data under the Data Protection Laws; and (ii) have appropriate technical and organisational

measures for the processing operations which ensure that mass and indiscriminate processing of personal data by or on behalf of public authorities in transit is not conducted.

## 8.2 Notification

Subject to Paragraph 8.3 (*Prohibition from notification*), where Supplier or any sub-contractor receives a legally binding request from any government, public authority and/or any other third party of any country (or anybody with delegated authority for any of them) for access to Unilever Personal Data (“**Disclosure Request**”), Supplier shall promptly notify Partner of the Disclosure Request, and such notification shall include information about the Unilever Personal Data requested, including the requesting authority, the legal basis for the request and the response provided. Supplier shall, using commercially reasonable endeavours, provide such reasonable assistance as Partner, or upon Partner’s request, Unilever requires in connection with the Disclosure Request, including in connection with the initiation of court or other legal proceedings by Partner or Unilever. Such assistance shall be at the requesting party’s reasonable cost.

## 8.3 Prohibition from Notification

If Supplier is prohibited from notifying Partner under the laws of the country of the requesting government, public authority and/or third party, Supplier shall use its commercially reasonable efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. Supplier agrees to document its commercially reasonable efforts in order to be able to demonstrate them upon request.

## 8.4 Review of Legality of Disclosure Request

Supplier shall reasonably cooperate with Partner or, at Partner’s request, Unilever in review, under the laws of the country of the requesting government, public authority and and/or third party, of the legality of the Disclosure Request.

## 9. INFORMATION AND AUDIT

- 9.1 Supplier shall comply with all reasonable requests or directions of Partner or Unilever to verify and evidence its compliance with its obligations under this Exhibit.
- 9.2 Partner or a Unilever Group Company may share information obtained via the above with any of the foregoing entities or its or their professional advisors, regulators or supervisory authorities and any recognised stock-exchange on which any of the foregoing entities is listed.
- 9.3 Without limiting other remedies, if a scan, audit or inspection reveals any Supplier non-compliance with its data protection obligations, Supplier shall promptly resolve, at its own cost and expense, such non-compliance and take appropriate measures to prevent re-occurrence.

## 10. PARTNER OBLIGATIONS

### 10.1 Partner shall:

- 10.1.1 ensure that its instructions for the Processing of Unilever Personal Data (including when it becomes aware of any breaches or non-compliances with Data Protection Laws at its end) shall comply with Data Protection Laws;

- 10.1.2 have responsibility for contracting with Unilever on Unilever's responsibility for the accuracy, quality, integrity, reliability and legality of the Unilever Personal Data it collects and the means by which it is obtained, collected and/or acquired.
- 10.1.3 contract with Unilever for Unilever to provide all necessary notices to Data Subjects and procure all necessary consents in order for Tungsten Network's Processing of Unilever Personal Data in connection with the Services to comply with notice / consent provisions of Data Protection Laws; and
- 10.1.4 contract with Unilever for Unilever to fulfil any obligations under Data Protection Laws to notify the Processing of Unilever Personal Data to the applicable data protection authority.

**APPENDIX A**  
**DATA PROCESSING ANNEXES**

## ANNEX 1

## TEMPLATE FOR DATA TRANSFER DETAILS

<b>Data exporter(s)</b>	<p><u>Name</u>: Unilever Business and Marketing Support AG and any other Unilever Group Company established in the EEA, UK, or Switzerland.</p> <p><u>Address</u>: Spitalstrasse 5, 8200 Schaffhausen, Switzerland.</p> <p><u>Contact person's name, position and contact details</u>: Peter Farrell, Global Privacy Director, peter.farrell@unilever.com.</p> <p><u>Activities relevant to the data transferred under these Clauses</u>: Unilever receives Services from Provider under this SOW that necessitate the transfer of Personal Data.</p> <p><u>Role (controller/processor)</u>: Controller.</p>	
<b>Data importer(s)</b>	<p><u>Name</u>: Genpact India Private Limited</p> <p><u>Address</u>: 12A (Ground Floor), Prakash Deep Building 7, Tolstoy Marg, New Delhi – 110001, India</p> <p><u>Contact person's name, position and contact details</u>:</p> <p><u>Activities relevant to the data transferred under these Clauses</u>:</p> <p><u>Role (controller/processor)</u>: Sub-Processor</p>	
<b>Categories of data subjects</b>	<b>Categories of personal data</b>	<b>Purpose(s) and Nature of the processing/transfer</b>
<p>Employees or personnel of Partner and Unilever and UGC and/or Unilever's customers;</p> <ul style="list-style-type: none"> <li>o Employees or personnel of the suppliers of Unilever and UGC.</li> <li>o Unilever's Users authorised to use the services.</li> <li>o Data subjects may be located globally.</li> </ul>	<p>Names</p> <p>Work e mail addresses, telephone numbers and e-mail addresses.</p>	<p>To perform the services (including support and access) provided to the Partner under the Agreement.</p>
<b>Frequency of the transfer (one-off or ongoing)</b>	Ongoing for the duration of the Services.	
<b>Data retention period (either an exact time period or criteria used to determine it)</b>	For the duration of the Services and thereafter as specified in the Agreement.	
<b>Restrictions and safeguards for sensitive data</b>	Please refer to Exhibit B ( <i>Information Security</i> ) of the Agreement.	
<b>Competent supervisory authority</b> (See Clause 13 of the Clauses.)	<p>The supervisory authority of the EU/EEA Member State where the data exporter is established (except as otherwise specified in Annex 4 (<i>UK International Data Transfer Addendum to the EU Standard Contractual Clauses</i>) and Annex 5 (<i>Swiss Addendum to the EU Standard Contractual Clauses</i>) of Appendix A (<i>Data Processing Annexes</i>) of Exhibit C(<i>Data Protection Provisions</i>) of the Agreement, concerning the UK and Switzerland, respectively).</p>	



<b>Governing law and choice of forum</b> <b>(See Clauses 17 and 18 of the Clauses.)</b>	The law of the Netherlands and the courts of the Netherlands (except as otherwise specified in Annex 4 ( <i>UK International Data Transfer Addendum to the EU Standard Contractual Clauses</i> ) and Annex 5 ( <i>Swiss Addendum to the EU Standard Contractual Clauses</i> ) of Appendix A ( <i>Data Processing Annexes</i> ) of Exhibit C ( <i>Data Protection Provisions</i> ) of the Agreement, concerning the UK and Switzerland, respectively).
<b>General or specific authorization of sub-processors (and specify time period for notifying the data exporter of new sub-processors)</b> <b>(See clause 9 of the Clauses.)</b>	The Controller has authorised the use of the following sub-processors: 1. Name: Mahendra NextWealth IT India Private Limited Address: #16, CPS Towers, Advaita Ashram Road, Salem -636004 Contact person's name, position and contact details: Prabhu Sundaram Velusamy, General Manager, prabhu.velusamy@mnxw.org Description of processing (including: (i) whether the authorisation is general or specific; and (ii) a clear delimitation of responsibilities in case several sub-processors are authorised): ...] <b>[Drafting note: update with list of approved sub-processors once Unilever approves.]</b>
<b>Technical and organizational measures (including any supplementary measures deemed necessary to provide an essentially equivalent level of protection to Personal Data, if applicable):</b>	Please refer to Exhibit B ( <i>Information Security</i> ) of the Agreement, as well as the supplementary measures specified in Annex 2 ( <i>Supplementary Measures</i> ) of Appendix A ( <i>Data Processing Annexes</i> ) of Exhibit C ( <i>Data Protection Provisions</i> ) of the Agreement.

## ANNEX 2

## SUPPLEMENTARY MEASURES

Pursuant to the transfer risk analysis conducted by the Parties, Supplier agrees to be subject to and/or implement the measures selected below:

<b><i>Contractual Measures</i></b>	
<input type="checkbox"/> Supplier shall notify any public authority making an access request if the request conflicts with the terms of the applicable Personal Data transfer mechanism.	<input type="checkbox"/> Supplier shall publish transparency reports on requests for disclosure to Personal Data it has received from government authorities to be made publicly available, or send such reports to Unilever directly on an annual basis.
<input type="checkbox"/> Supplier shall enquire of any public authority making an access request for Personal Data whether it is cooperating with EEA Member State authorities in relation to the matter.	<input type="checkbox"/> Supplier shall assist data subjects in exercising their rights in the third country jurisdiction by providing reasonable assistance.
<input checked="" type="checkbox"/> Supplier warrants that it has not purposefully created any technical backdoors or other internal processes to facilitate government access to Personal Data, nor is it required to do so by law applicable in the third country.	<input type="checkbox"/> Supplier shall regularly send an encrypted message informing Unilever that it has not received a government request to disclose Personal Data.
<input checked="" type="checkbox"/> Supplier shall cooperate with Unilever in the event that an EEA supervisory authority or an EEA court of competent jurisdiction determines that the transfer must be subject to specific additional safeguards (including, but not limited to, specific technical and organizational measures).	<input type="checkbox"/> Supplier shall conduct a TIA on any onward transfers and is permitted to proceed with such transfers only if it concludes that the Personal Data will receive essentially equivalent protection in the third country (including through the implementation of supplementary measures).
<input type="checkbox"/> Supplier shall monitor changes in the third country and ensure that this TIA is updated to reflect relevant changes.	
<input type="checkbox"/> Other contractual measures ( <i>please specify</i> ):	
<b><i>Organizational Measures: as agreed in Exhibit B (Information Security)</i></b>	
<input type="checkbox"/> Other organizational measures ( <i>please specify</i> ):	
<b><i>Technical Measures: as agreed in Exhibit B (Information Security)</i></b>	
<input type="checkbox"/> Other technical measures ( <i>please specify</i> ):	

**ANNEX 3**  
**TRANSFER PROVISIONS**  
**EU STANDARD CONTRACTUAL CLAUSES**  
**MODULE 3: PROCESSOR-TO-PROCESSOR**

**STANDARD CONTRACTUAL CLAUSES**

**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) 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*

***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 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***

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**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.

**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 I. 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 (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:

- (a) 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;
- (b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (c) 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
- (d) 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) **SPECIFIC PRIOR AUTHORISATION:** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least the time period set forth in Section 6 prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex I. The Parties shall keep Annex I up to date.
- (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. 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 I 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 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) 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.
- (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;
  - (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 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 the Netherlands.

*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 the Netherlands.
- (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.

**ANNEX 4**

**UK INTERNATIONAL DATA TRANSFER ADDENDUM TO**

**THE EU STANDARD CONTRACTUAL CLAUSES<sup>1</sup>**

**PART 1: TABLES**

**Table 1: Parties**

<b>Start date</b>	On or after <span style="background-color: yellow;">                    </span>	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Please refer to the UK entities specified in the Agreement, and/or the UK affiliates of the entities specified in the Agreement, as applicable.	Please refer to the non-UK entities established in non-adequate third countries specified in the Agreement, and/or the non-UK affiliates of the entities specified in the Agreement established in non-adequate third countries, as applicable.
<b>Key Contact</b>	Genpact: <span style="background-color: yellow;">Anand Kumar</span>	

**Table 2: Addendum EU SCCs**

<b>Addendum EU SCCs</b>	<input checked="" type="checkbox"/> <b>The version(s) of the Approved EU SCCs which this UK Addendum is appended to, including the Appendix Information detailed below.</b>
-------------------------	---

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

---

<sup>1</sup> Version B1.0, in force 21 March 2022. This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

<u>Annex I.A: List of Parties:</u> Please refer to [insert ref] (Data Transfer Details) of this SOW.
<u>Annex I.B: Description of Transfer:</u> Please refer to [insert ref] (Data Transfer Details) of this SOW.
<u>Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:</u> Please refer to [insert ref] (Data Transfer Details) of this SOW.
<u>Annex III: List of Sub processors (if applicable):</u> Please refer to [insert ref] (Data Transfer Details) of this SOW.

**Table 4: Ending this UK Addendum when the Approved Addendum Changes**

<b>Ending this UK Addendum when the Approved Addendum changes</b>	<p>Which Parties may end this UK Addendum as set out in Section 19:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
---	---

## PART 2: MANDATORY CLAUSES

### Entering into this UK Addendum

- Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
- Although Annex I.A. and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this UK Addendum

- Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.



Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this UK Addendum has been entered into.

## **Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

## **Incorporation of and changes to the EU SCCs**

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - (a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - (b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - (c) this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
  - (a) References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;
  - (b) In Clause 2, delete the words:
 

"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";
  - (c) Clause 6 (Description of the transfer(s)) is replaced with:
 

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B. where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

- (d) Clause 8.7(i) of Module 1 is replaced with:  

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- (e) Clause 8.8(i) of Modules 2 and 3 is replaced with:  

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
- (f) References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- (g) References to Regulation (EU) 2018/1725 are removed;
- (h) References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- (i) The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- (j) Clause 13(a) and Part C of Annex I are not used;
- (k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- (l) In Clause 16(e), subsection (i) is replaced with:  

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- (m) Clause 17 is replaced with:  

“These Clauses are governed by the laws of England and Wales.”;
- (n) Clause 18 is replaced with:  

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- (o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

### **Amendments to this UK Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
  - (a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - (b) reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the UK Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - (a) its direct costs of performing its obligations under the UK Addendum; and/or
  - (b) its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

## ANNEX 5

### SWISS ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

For transfers of Personal Data originating in Switzerland, the EU Standard Contractual Clauses shall be amended in accordance with statement of the Swiss Federal Data Protection and Information Commissioner (“**FDPIC**”) of 27 August 2021.<sup>1</sup> In particular:

- A. The FDPIC shall be the competent supervisory authority insofar as the transfer is governed by the Swiss Federal Act on Data Protection (“**FADP**”) (Clause 13);
- B. The law of the country specified in the EU Standard Contractual Clauses shall be the governing law (Clause 17);
- C. The courts of the country specified in the EU Standard Contractual Clauses shall be the choice of forum (Clause 18), but this shall not exclude data subjects in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c); and
- D. The EU Standard Contractual Clauses shall protect the data of legal entities in Switzerland until the entry into force of the revised FADP.

---

<sup>1</sup> Available for direct download at:  
<https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf>.

## EXHIBIT B

### INFORMATION SECURITY REQUIREMENTS

#### 1. INTRODUCTION

This Exhibit B sets out Information security requirements which Supplier shall adhere to in respect of delivering the Supplier Services to Company with effect from the SOW Effective Date, unless otherwise specified or agreed to by the parties. The definitions set forth in the Agreement, including without limitation the Data Protection Provisions in Exhibit A, shall apply herein.

#### 2. DEFINITIONS

In this Exhibit, the following additional definitions apply, unless the context otherwise requires:

**“Customer and/or Customer Client Data”** means Unilever Personal Data as defined in Exhibit C and Confidential Information as defined in the Agreement.

**“Customer and/or Customer Client Systems”** means the equipment, Software and other electronic, computer and information communications technology devices and equipment owned, supplied, operated and/or developed by any member of the Customer and/or Customer Client Group and/or any of its subcontractors as varied, updated and renewed from time to time including all networks, servers, hosted applications and data centres and any equipment contained therein.

**“Customer Security Team”** means the Customer information protection team, or within the context of this Exhibit B, from which the appropriate points of contacts for activities defined in this Exhibit will be communicated to Supplier, including updates to organisation, throughout this Agreement.

**“ISO 27001”** means ISO 27001:2013, an information security standard that was published on 25 September 2013 by the International Organization for Standardization and the International Electrotechnical Commission, as may be amended from time to time.

**“ISO 27001 Audit Results”** shall have the meaning set out in Paragraph 3(c) (*Standards Compliance*) of this Exhibit B.

**“ISO 27002”** means ISO/IEC 27002, means document that provides a reference set of generic information security controls including implementation guidance published by the International Organization for Standardization and the International Electrotechnical Commission, as may be amended from time to time.

**“Personal Data Breach** - personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes.

**“Supplier Information Security Representative/SPOC”** means an employee nominated by Supplier to be a single point of contact in respect of Supplier’s obligations set out in this Exhibit B for the Term.

**“Supplier Systems”** include all equipment, devices, applications, networks and transmission, cloud and other systems controlled by Supplier.

“**Reviewer**” shall have the meaning set out in Paragraph **Error! Reference source not found.** (*Security Review*) of this Exhibit B.

“**Security Incident**” means an information protection incident relating to Confidential Information which occurs where (i) Confidential Information is intentionally or unintentionally disclosed to an unauthorised environment or recipient, or (ii) there is an unauthorised access of Customer and/or Customer Client Data, Systems and/or Networks, resulting in inappropriate use, falsification or an impact on availability. For the avoidance of doubt, a Security Incident is not a Personal Data Breach.

“**Security Review**” shall have the meaning set out in Paragraph **Error! Reference source not found.** (*Security Review*) of this Exhibit B.

“**Statement of Applicability**” means the statement defined under ISO 27001, which requires organisations to produce a Statement of Applicability that lists the controls that have been selected to treat identified risks, and provides a justification for the inclusion of those controls, regardless of whether they have been implemented or not, and the status of implementation for the selected controls, and to link to relevant documentation showing how each control is (or will be) implemented.

“**VDI**” shall have the meaning set out in Paragraph **Error! Reference source not found.** (*Access Arrangements*) of this Exhibit B.

### 3. **STANDARDS COMPLIANCE**

- (a) Supplier shall be ISO 27001 certified and its Statement of Applicability shall apply to the Services as defined in this Agreement. The scope of ISO 27001 certification shall include all the sites and teams which are delivering services to Company and/or Unilever.
- (b) Supplier shall also adopt the ISO 27002 code of best practice for information security.
- (c) Supplier shall provide to Customer the results of Company’s latest ISO 27001 certification audit (“**ISO 27001 Audit Results**”) and its Statement of Applicability promptly upon request by Company. Supplier shall provide the ISO Certificate, a summary of the certification audit results including observations and mitigation plans within 30 days of obtaining such certification. Supplier shall also obtain and confirm to Customer ISO 27001 re-certification on an annual basis within 30 days of receipt of the re-certification.

### 4. **SECURITY ORGANISATION**

- (a) Supplier shall have an information security function, which has responsibility for ensuring good practice in relation to information security across the Supplier Group and in relation to the provision of the Services.
- (b) The head of Supplier's information security function shall be responsible for information security across the Provider Group and shall ensure that Provider's information security policies are at all times observed by Provider in the course of providing the Services.

- (c) Supplier shall appoint a single point of contact for information security who is independent of, is not a part of and does not report into the project/operations team.
- (d) Supplier shall ensure that Supplier Personnel with access to Company and/or Company Data are made aware of the obligations under this Exhibit B.
- (e) Supplier shall ensure that adequate Information Security and Privacy training are imparted on annual basis to maintain compliance with the agreed contractual obligations and Supplier's security policies.

## 5. **SERVICE LEVELS, GOVERNANCE AND REPORTING**

- (a) The Supplier Information Security Representative shall:
  - (i) arrange security governance reviews with Company and/or Company Client at an agreed frequency, which shall be no less than monthly; and
  - (ii) ensure an effective security organisation with embedded security processes across the Services provided to Company and/or Company Client. The Provider Information Security Representative shall clearly communicate points of contact and escalation paths to Company and/or Company Client to ensure priority security concerns are addressed.
- (b) Supplier shall continuously assess security risks to the Services and report monthly with detailed assessment and recommended mitigation controls and actions to the Customer Security Team. Any urgent risks must be highlighted by the Supplier Information Security Representative to Customer immediately on identification of such urgent risks.

### **A. Penetration Testing**

- (i) Upon agreement with Supplier not to be unreasonably withheld a Third Party (Third Party here shall mean industry known third party vendors of the Provider) may perform penetration testing on the Provider's systems at an enterprise level no more than once every twelve (12) months and provide high-level executive summary of the results to Company upon request. In the event that the penetration testing conducted discovers vulnerabilities in Provider's system, resulting in the Provider's level of compliance to this Exhibit to be non-compliant, Provider and Company shall mutually agree on the additional penetration testing and the Third Party shall be permitted to perform a second penetration test following the remediation of these vulnerabilities focusing on those vulnerabilities discovered from the initial penetration testing and provide high-level executive summary of the results to Company upon request.
- (ii) All public facing systems and services including but not limited to applicable web application, database and operating system used for providing Services to Company and/or Buyer must be penetration tested by the Provider before go live date (or as agreed in writing), and on an annual basis thereafter.



**B. Vulnerability Scanning**

- (i) Supplier shall comply with the Supplier's continuous vulnerability management procedures, to the extent applicable to the scope of the Services under the Agreement and while working on the Company and/or Company Client Systems's or accessing Company and/or Company Client Data or network, Supplier shall comply with the Unilever's Continuous Vulnerability Management Standard.
- (ii) Upon identification of vulnerabilities on Provider' maintained IT Systems, Supplier will remediate such vulnerabilities in accordance with a mutually agreed remediation schedule. A decision not to remediate any vulnerabilities must be subject to mutual agreement with Company and/or Company Client.

**C. Infrastructure and Application Testing**

- (i) Supplier shall arrange for appropriate infrastructure and application security tests to take place and the scope and frequency of such tests shall be agreed between the Provider and Company in line with the risk profile of the Customer Systems in scope of the Agreement and documented as a formal testing schedule.
- (c) Supplier shall work with Company to align risk values (including data classification) and control deployment to ensure Company requirements for data confidentiality, integrity and availability are met.

**6. SECURITY INCIDENT MANAGEMENT**

- (a) Supplier shall ensure that Supplier Personnel are trained and aware of Company's Security Incident management procedures as set forth in Section 6(f) below.
- (b) Supplier shall inform Company, in accordance with the agreed Company Incident management procedures set out in Section 6(f) below, of any known or suspected Security Incident, or any other risk, that affects, or has the potential to affect, the security of Customer and/or Customer Client Data.
- (c) Supplier shall provide confirmation to Customer within thirty (30) days of execution of the SOW that all its Approved Sub-Contractors are bound to notify Supplier of any actual or suspected Security Incident or, in the absence of such confirmation, what steps it proposes to take to minimise the risk of any actual or suspected Security Incident not being notified. Provider must notify Customer and/or Customer Client promptly upon receipt of such notification from an Approved Sub-Contractor.
- (d) Supplier shall promptly report in writing to Customer any issue or potential issue of which Provider or any Approved Sub-Contractor is or becomes aware which has or may have an adverse effect on the provision of the Services or on the availability, confidentiality or integrity of Customer and/or Customer Client Data or Customer and/or Customer Client Systems; In the event of such a report, Supplier shall, procure that Approved Sub-Contractors shall, cooperate fully with Supplier to resolve any such adverse effects.

- (e) Supplier shall promptly report to Customer all identified attempts (which are successful) of which it becomes aware by unauthorised persons (including unauthorised persons who are Provider Personnel) either to gain access to or interfere with Customer Client Data.
- (f) If Supplier becomes aware of or reasonably suspects the occurrence of a Personal Data Breach, Provider shall follow the notification process set forth in 5 of the Data Protection Addendum in Exhibit C.

If Supplier becomes aware of or reasonably suspects the occurrence of a Security Incident, it shall without undue delay and in any event within twenty-four (24) hours of the identification of any such Security Incident:

1. notify Customer, providing all relevant information, including:
    - a. the nature of the Security Incident;
    - b. any existing or anticipated involvement of regulatory authorities; and
    - c. any measures taken, or that Supplier recommends, to deal with the Security Incident and/or its adverse effects, and
  2. investigate and report to Customer on the cause of the Security Incident, including proposed corrective action within 36 hours after notification of the Security Incident and provide Customer with detailed related information; and
  3. take all reasonable steps itself and also provide all reasonable assistance to Customer (at Customer's reasonable cost, save where the Security Incident was caused solely by Provider and/or any of its subcontractors), to remediate or mitigate any actual or potential damage from a Security Incident (including reasonably supporting any Customer or Client's response plan) and to prevent re-occurrence (which may include removal of service personnel).
- (g) Supplier shall provide all reasonable co-operation with any investigation relating to security which is carried out by or on behalf of Customer and, if requested by Customer, Provider shall, for the purposes of the investigation:
    - (i) make any Supplier Personnel identified by Customer and/or Customer Client available to be interviewed by or on behalf of Customer and/or Customer Client for the purposes of the investigation; and
    - (ii) provide all documents, records or other material/information extracted from such documents/records of any kind which may reasonably be required for the purposes of the investigation. Customer shall have the right to retain copies of any such material to the extent required for the purposes of the investigation.

All suspected or actual incidents pertaining to the scope of service of this agreement shall be notified to [CSIRT@genpact.com](mailto:CSIRT@genpact.com).

## 7. ACCESS MANAGEMENT

- (a) Where Services require an interface or other connection to Customer and or Customer Client Systems, Supplier shall be responsible for validating the identity of Supplier Personnel involved in providing the Services. Supplier must keep Customer and or Customer Client apprised of the names of Supplier Personnel and the required and actual levels of access to Customer and or Customer Client Data (including sub-contractors).
- (b) Supplier shall ensure that Supplier Personnel at all times, have the minimal required system access to carry out their duties. Supplier shall not use shared privileged accounts.
- (c) Supplier shall ensure that access to Customer and/or Customer Client Systems is subject to the industry standard security controls and that failure by Supplier Personnel to comply is subject to appropriate disciplinary action.
- (d) Supplier shall ensure that relevant Supplier Personnel are assigned a set of access privileges to allow them to read or change particular information or systems in accordance with their specific role requirements, any changes to these privileges shall be undertaken in accordance with agreed Change Control processes.
- (e) Supplier shall ensure all Customer and/or Customer Client Data is logically separated so that no other client of any Provider Group shall be able to access the Customer and/or Customer Client Data physically or logically.
- (f) Supplier shall apply industry standard physical security controls where Customer and/or Customer Client Data is held.
- (g) Provider shall keep an inventory of Provider's physical sites and IT systems, where Customer and/or Customer Client Data is stored, and whether in physical and/or electronic form.

## 8. ASSET MANAGEMENT

### (a) Asset Inventory

If Supplier stores Customer and/or Customer Client Data as part of a Service Line, Provider shall maintain an inventory of all media on which Customer and/or Customer Client Data is stored. Access to the inventories of such media is restricted to Provider Personnel authorized in writing to have such access.

### (b) Asset Handling

- (i) Supplier classifies Customer and/or Customer Client Data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

- (ii) Supplier imposes restrictions on printing Customer and/or Customer Client Data and has procedures for disposing of printed materials that contain Customer and/or Customer Client Data.
- (iii) Supplier Personnel must obtain Provider authorization prior to storing Customer and/or Customer Client Data on portable devices, remotely accessing Customer and/or Customer Client Data, or processing Customer and/or Customer Client Data outside Provider's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Customer and/or Customer Client Data from Provider's facilities.

## 9. POLICY AND PROCESS

- (a) Supplier shall have documented corporate information security policies and standards approved at a sufficiently senior level within Provider organisation to ensure corporate compliance. The information security policy shall apply to all Supplier Personnel and their use of Customer and/or Customer Client Data and Customer and/or Customer Client Systems from Provider Systems. For the avoidance of doubt, if Supplier is working at Customer and/or Customer facilities or on Customer and/or Customer Client Systems, Provider will adhere to applicable Customer and/or Customer Client's policies as notified in writing in advance to Supplier.

## 10. SECURITY REVIEW

(a) Supplier and/or its Approved Sub-Contractors (as applicable) shall permit Customer and/or Customer Client Personnel, authorised representatives and any party to whom Customer and/or Customer Client is legally obliged to provide access or audit rights ("Reviewers"), to review and assess Supplier's and/or its Approved Sub-Contractors (as applicable) compliance with the obligations set out in this Exhibit B ("Security Review").

(b) For the avoidance of doubt, Supplier's compliance with Data Protection Legislation is subject to the provisions of Exhibit A (*Data Protection Provisions*). Any review which indicates security issues in respect of Supplier's processing of Personal Data must be remedied in accordance with the provisions of Exhibit A (*Data Protection Provisions*).

(c) The Reviewers shall be entitled to, in respect of Supplier, and/or its Approved Sub-Contractors, access the premises controlled by them, extract any Customer and/or Customer Client Data held on their Systems, inspect their security risk management controls and procedures, and interview Supplier Personnel in order to assess compliance with the obligations set out in this Exhibit B.

(d) Subject to Paragraph 10(e), Customer shall be entitled to conduct a Security Review in accordance with this Paragraph 10 no more than once per annum, unless a Security Review upon request is reasonable, such as following a Security Incident and/or Personal Data Breach. In such case Customer and/or Customer Client may exercise the rights under this Paragraph 10 upon service of no less than twenty-four (24) hours (unless otherwise agreed in writing) advance, written notice. Where practicable, the Security Review will be performed via webinar and other remote communications methods.

(e) Supplier and/or its Approved Sub-Contractors (as applicable) shall remediate any failures identified by the Security Review as agreed with Customer including developing a comprehensive remediation solution for identified gaps. The cost of remediation shall be borne by Supplier and/or its Approved Sub-Contractors (as applicable).

(g) Notwithstanding any language to the contrary set forth herein, all audits conducted by Customer and/or Customer Client and its auditors pursuant to this Exhibit shall be subject to the following conditions:

- (i) Customer and/or Customer Client's auditors shall execute and deliver non-disclosure agreement(s) reasonably acceptable to Provider;
- (ii) audits shall not be conducted by Supplier Competitors;
- (iii) audits shall be conducted during regular business hours;
- (iv) except for audits conducted by regulators, audits may not be conducted more than once per calendar year with a written notice of thirty (30) days; and
- (v) during audits of remote work locations, Customer and/or Customer Client will not record or otherwise capture any sounds or images or personal information of Provider Personnel, and Customer and/or Customer Client will not have direct physical access to remote work locations.

The audit requirements and obligations relating to Approved Sub-Contractors under this Paragraph 10 apply only to Approved Sub-Contractors whose services which are material to the provision of the Services. In addition, the parties agree that these audit rights do not include the right to install audit tools, the right to conduct ethical hacking, penetration testing or vulnerability testing of Approved Sub-Contractors' systems or networks.

#### **11. SHARED SERVICES**

- (a) Supplier Personnel delivering the Services shall work in databases and other systems that are logically segregated from Supplier Provider's other customers, including Customer and/or Customer Client Competitors.
- (b) Supplier shall ensure that all Customer and/or Customer Client Data is logically segregated from all other data and information held by Provider and any of its Approved Sub-Contractors, either for itself or on behalf of its other customers, including any competitors of Customer and/or Customer Client.
- (c) Supplier must logically segregate the network that processes Customer and/or Customer Client Information, including printing facilities, from Provider's other networks.

#### **12. BUSINESS CONTINUITY MANAGEMENT**

Supplier will have and maintain adequate *Disaster Recovery and Business Continuity* plans, including IT service continuity, which are tested and approved at least annually. A summary of the successful results of such testing will be provided to Customer upon request.

#### **13. DATA AVAILABILITY CONTROL:**

Supplier shall implement and maintain appropriate and adequate security measures and procedures in order to ensure Confidential Information and/or Customer and/or Customer Client Data availability, including procedures to ensure that Confidential Information and/or Customer and/or Customer Client Data are protected from accidental destruction or loss, including against loss that may result from a power shortage or interruptions in the power supply.

**14. BACKUP, RETENTION, AND RECOVERY:**

Supplier shall implement and maintain appropriate and adequate backup and recovery security measures and procedures in order to ensure data availability in the event of loss of data or information systems from any cause. Backups must be tested periodically.

**15. OBLIGATIONS ON TERMINATION**

- (a) Upon termination or expiry of the Agreement, Supplier shall, to the extent applicable, promptly and securely, within thirty (30) Business Days of that termination/expiry date, either (as directed by Customer and/or Customer Client):
  - (i) destroy Customer and/or Customer Client Data in Supplier's (including subcontractors') possession or control followed by producing necessary evidence. However, Supplier shall retain and properly store during the Term of the Agreement and following termination or expiry for at least seven (7) years thereafter, all financial or other information where required by applicable law.

## APPENDIX A

### CUSTOMER AND/OR CUSTOMER CLIENT CYBER SECURITY INCIDENT REPORTING & INVESTIGATION GUIDELINES FOR 3<sup>RD</sup> PARTY PROVIDERS

Customer and/or Customer Client requires that all cybersecurity and business continuity incidents are promptly reported and appropriately investigated. “**Incident**” means any event which impacts or has the potential to impact Customer and/or Customer Client’s assets, including (but not limited to) our information, brands, IT systems, employees and our business processes/objectives.

This document provides our 3<sup>rd</sup> parties with clear guidance on Customer and/or Customer Client’s expectations as to when and how they will report incidents, and how incidents affecting Customer and/or Customer Client assets will be investigated and managed. Detail is also provided on the roles and respective responsibilities for Customer and/or Customer Client and our 3<sup>rd</sup> party stakeholders, including key requirements for forensics investigations where required.

The term Cybersecurity for the purpose of this document is defined as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Such controls are in place to prevent/limit harm to Customer and/or Customer Client’s systems and data, as well as to individuals or brands in financial, intellectual or reputational terms or any other loss as an impact of the incident.

#### 1. INTENDED AUDIENCE

This document is for providers with access to or who support Customer and/or Customer Client systems, or who process Customer and/or Customer Client data/information. It is expected that specific IT and/or Cybersecurity roles at the Provider will fulfil the responsibilities described, with support from other resources, e.g., business continuity experts, crisis management experts.

#### 2. WHAT TO REPORT

All Providers engaged by Customer and/or Customer Client are required to report actual / confirmed breaches or compromises affecting Customer and/or Customer Client data, or environments where Customer and/or Customer Client data is stored and/or processed.

Examples of such security events may include (but are not limited to) any of the following:

*Compromised computing resources, which includes:*

- *System (OS) account compromises*
- *User account compromises*
- *Point-of-sale intrusions*

*Email-facilitated compromise resulting from:*

- *Unsolicited Commercial Email (UCE), more commonly known as “spam”*
- *Phishing Emails seeking recipient's user credentials or personal information*

*on web applications through:*

- *Cross site scripting (XSS)*
- *SQL injection*
- *DDoS attacks*

*Network and network resource incidents, including:*

- *Network scanning activity*
- *Denial of Service attacks*

*Resource misconfiguration incidents, including:*

- *Attacks on open proxy servers and anonymous FTP servers*
- *Vulnerable software configurations that may result in a future compromise*
- *Abuse via web forms and blog sites*
- *Misuse of licensed resources Malware related attacks such as:*
- *Ransomware*
- *Worm infections to significant number of users*

*Other types of incidents:*

- *Copyright Infringement Reports*
- *Misuse of privileges by rogue employee or other insiders*
- *Physical Loss or Theft of Equipment*
- *Major business disruption (Disaster Recovery scenario)*

### **3. WHEN TO REPORT IT**

Customer and/or Customer Client requires that providers report incidents through the appropriate channel in accordance with the timescales set out within the relevant contractual agreement.

The table below in Appendix B provides an indication of how Customer and/or Customer Client will internally classify the severity of cybersecurity incidents. This information is provided to aid providers in accurately reporting incidents involving Customer and/or Customer Client data or systems. The Customer and/or Customer Client ISOC Manager will make the ultimate decision on Customer and/or Customer Client's classification with respect to incident priority

### **4. HOW TO REPORT IT**

As a general principle, the Supplier must *directly* inform Customer CSIRT of any incidents or investigations affecting Customer and/or Customer Client systems or data. Contact must be via email and a supporting phone call using the contact details provided below.

Security Incidents known by Provider arising from Customer Systems or Personnel are reportable at [CSIRT@genpact.com](mailto:CSIRT@genpact.com).

All emails to CSIRT must have a subject line that starts with the words "PROVIDER NOTIFICATION" and include Supplier's normal Customer and/or Customer Client business relationship owner in the CC field.

Providers must always ensure that they provide CSIRT with the name and contact details of the Provider's normal Customer and/or Customer Client business contact.

This direct contact will allow Customer and/or Customer Client to provide a prompt response, enable appropriate investigation and to fulfil its obligations in respect of regulatory notification under national



data protection law and multinational regulations such as the European Union's General Data Protection Regulations which came into effect in May 2018.

Notification should also be provided the Provider's key Customer and/or Customer Client business contact. The Customer and/or Customer Client business contact will then take appropriate internal action to notify additional Customer and/or Customer Client stakeholders as necessary.

### **Legally Reportable Incidents**

This guideline does not supersede any local, national or international legal requirements regarding incident notification and does not absolve Providers from any other compliance responsibilities to notify different Customer and/or Customer Client stakeholders.

### **Incident Investigation Approach**

Customer and/or Customer Client expects all providers to conduct their investigations in line with their own formally documented procedures. Customer and/or Customer Client may request further information in relation to an incident in order to seek assurance that adequate investigation and remediation measures have been undertaken. Customer and/or Customer Client expects all such investigations to be treated and handled as confidential with communication conducted on a strictly need to know basis.

The responsibility for an investigation by a Provider should be handled by a technically competent "Cyber Security Investigation Lead" or equivalent role. The Provider's Cyber Security Investigation Lead is responsible for undertaking a thorough incident analysis, including use of forensic techniques where appropriate, and identifying those corrective actions required. The Cyber Security Investigation Lead is required to provide a completed root cause analysis to their Customer and/or Customer Client business contact (or to the Customer and/or Customer Client ISOC for incidents involving personal data.)

Customer and/or Customer Client reserves the right to engage with the affected Provider and actively support any cyber incident investigation where justified by the:

- 1) Criticality of the Customer and/or Customer Client data affected.
- 2) Impact to the Customer and/or Customer Client operations.
- 3) Potential reputational impact to Customer and/or Customer Client.
- 4) Impact on Customer and/or Customer Client's compliance with government and regulatory requirements.

**APPENDIX B****CUSTOMER AND/OR CUSTOMER CLIENT INCIDENT CLASSIFICATION**

The below table is provided to the Provider for information purposes only. It sets out the classification approach Customer and/or Customer Client uses internally for incidents.

Category	Definition
Crisis	<ul style="list-style-type: none"> <li>• Third party is no longer able to control the critical external dynamics of the situation.</li> <li>• An anticipated loss of control where Customer and/or Customer Client is no longer able to control the critical external dynamics of the situation.</li> <li>• A situation where a group of Customer and/or Customer Client managers (with sufficient authority) agree upon the necessity of convening a formal crisis team to protect the interests of the company.</li> <li>• A breach or loss of employee or consumer data occurs on a large scale across multiple geographies, that requires public disclosure, generates large scale global media interest and engagement of internal communications channels.</li> </ul>
Critical / P1	<ul style="list-style-type: none"> <li>• Confirmed compromise of a Crown Jewel asset or systems holding Restricted data.</li> <li>• Unrestricted external exposure of Restricted Customer and/or Customer Client data.</li> <li>• Security event leading to a loss of service on an SC1 system.</li> </ul>
High / P2	<ul style="list-style-type: none"> <li>• Confirmed compromise of system holding Confidential data (Personal or Sensitive Personal) or eCommerce systems.</li> <li>• Unrestricted external exposure of significant amount of personal / sensitive personal data, or authentication credentials to systems holding this information.</li> <li>• Security event leading to a loss of service on an SC2 system.</li> <li>• New malware infection rated to have significant impact by Threat Intel.</li> </ul>
Medium / P3	<ul style="list-style-type: none"> <li>• Suspected compromise of systems holding Restricted, Sensitive Personal or Personal data.</li> <li>• Confirmed compromise of systems holding Internal Customer and/or Customer Client data or exposure of internal Customer and/or Customer Client data.</li> <li>• Security event leading to a loss of service on an SC3 or SC4 system.</li> <li>• Known malware infection of more than 10 client devices.</li> </ul>
Low / P4	<ul style="list-style-type: none"> <li>• Suspected compromise of any Internal Customer and/or Customer Client data.</li> <li>• Known malware infection up to 10 client devices.</li> </ul>

## **Exhibit C**

### **Flow-Down Provisions**

#### **Subcontracts:**

Supplier acknowledges and agrees to be fully responsible and liable on behalf of any subcontractor engaged by Supplier in order to perform any part of the Services, provided such subcontractors are preapproved by Company in writing before being assigned any work under this Agreement.

#### **Divestment:**

If any Company/Client entity or Company/Client affiliate entity, division or business is to cease being part of the Company /Client Group ("**Departing Business**"), Company/Client may require, in each instance, that the Departing Business continues to receive and Supplier shall provide, the Services under and in accordance with the SOW and at no extra charge for a period of up to 24 months (subject to the term if the SOW) from the date of departure (the "**Divestiture Period**"), either by:

- onward supply by Customer to the Departing Business via a transitional services agreement between Customer and the Departing Business; and/or
- supply by Supplier shall to the Departing Business.

For the required Divestiture Period the Departing Business is deemed to continue as a Customer/Client affiliate for purposes of applying relevant statement of work's terms.

#### **Disclosures:**

A "Financial Distress Event" will be deemed to occur if Company or its Client reasonably believe that there are issues with Company's financial standing which will or are likely to prejudice Company's ability to perform its obligations under this SOW. Without prejudice to any other rights or remedies of Company or its Client, upon the occurrence of a Financial Distress Event, Company or its Client shall have the right to require Company to: a. provide such relevant financial information (given the nature of the Financial Distress Event) relating to Company which is publicly available as Company or its Client may reasonably require (which Company shall promptly provide); and/or b. arrange a meeting between Genpact and/or its Client's relevant Procurement Director and Company's Commercial Director whom Company shall make available for this purpose, as soon as reasonably practicable, in order to provide Company and/or its Client with reasonable comfort of Company's continuing financial stability and determine whether a service continuity plan is required.

#### **Recordkeeping and Audit Rights:**

Supplier/Company will cooperate and promptly provide to Customer and the Client all documentary proofs of compliance as may be required for audit, inspection or review related to the Services provided by Supplier to Customer or its clients. In addition, Supplier must provide access, upon reasonable notice from Customer or Client (which may be immediate access if the circumstances appropriately require), to the Supplier/Company's applicable offices, facilities, personnel and records to allow Customer and/or Client and/or their agents to verify that Supplier is in compliance with the terms of the relevant order and to otherwise conduct operational and financial audits/inspections relating to this SOW. Supplier /Company shall cooperate with Customer and/or Client and/or their agents in respect of any such audit or inspection.

**Termination:** (please note the UL-Genpact agreement has multiple termination triggers. Therefore Genpact/Quess should have wide termination rights as well. No termination fees (termination for convenience on 30 days' notice).

## **EXHIBIT D**

### **1. CLIENT DATA, IT SERVICES**

#### **1.1 Client Business Data**

- (a) All Client Business Data is to be considered Confidential Information of Client.
- (b) Only Client and/or a UGC and/or a Client Affiliate will have the right to determine how Client Business Data is used, disclosed and/or commercialised by any person, in whole or in part (whether substantial or insubstantial). Use of Client Business Data includes copying, extraction, and transmission.
- (c) Supplier/Company and each Supplier/Company Group Company and each Supplier/Company Affiliate must only use or disclose Client Business Data in accordance with the terms of the relevant Supplement and only to the extent:
  - (i) necessary for the provision of goods and/or performance of the Services under a Supplement; and/or
  - (ii) required by Applicable Legislation.
- (d) At Supplier/Company's written request or otherwise Client may (at its discretion) give written authorisation to Supplier/Company or any Supplier/Company Group Company or any Supplier/Company Affiliate to use or disclose Client Business Data for purposes other than as permitted in the preceding clause, subject to any conditions which may be imposed by Client in writing from time to time. Any such authorisation must be documented in the form of a Data Use Annex.
- (e) Prior to disclosing or granting access to Client Business Data to a third party, Supplier/Company shall ensure that it has a direct written contract with such third party that reflects the terms of this SOW and Agreement and does not permit any further sub-disclosure or sub-grant of access to Client Business Data.
- (f) Unless expressly permitted in a Supplement and/or a Data Use Annex, Special Client Business Data must only be accessed (and Client Derived Data that would be Special Client Business Data on creation must only be created) on IT Systems that Client controls ("Controlled Systems") and Supplier/Company (and/or any Supplier/Company Group Company and/or any Supplier/Company Affiliate) must not make copies of Special Client Business Data outside of Controlled Systems, whether in physical and/or electronic form.
- (g) Client may require additional contractual, technical and operational controls in respect of any Special Client Business Data. Such additional controls will be documented and agreed in a Data Use Annex.
- (h) Supplier/Company must ensure that each member of the Supplier/Company Personnel who has access to Client Business Data:
  - (i) is informed of the confidential nature of Client Business Data generally and the sensitive nature of any Special Client Business Data;
  - (ii) only accesses and/or uses Client Business Data to the extent strictly necessary for the performance of that Supplier/Company Personnel's duties;

(iii) is aware of Supplier/Company's obligations with regard to Client Business Data and Special Client Business Data under this Agreement, including the relevant Supplement and any relevant Data Use Annex;

(iv) is trained in all relevant procedures and guidelines with regard to the processing of Client Business Data.

(i) Supplier/Company must deal promptly and properly with all enquiries from Client relating to the use and disclosure of Client Business Data. Supplier/Company must promptly comply with any request from Client requiring Supplier/Company or any Supplier/Company Group Company and/or any Supplier/Company Affiliate to amend, delete, destroy, transfer, remove or return Client Business Data (or any part thereof) and to certify, by signature of a director, that this has been done.

(j) Supplier/Company must not delete or destroy any Client Business Data (including backups and copies) without Client's prior written consent or instructions to do so unless such deletion is required by this Agreement, the relevant Supplement or Client Policies. Supplier/Company must ensure that if Supplier/Company deletes, destroys or otherwise disposes of any Client Business Data, such disposal takes place in a secure manner such that the Client Business Data is not recoverable, and is in accordance with any relevant Client Policy.

(k) If in the reasonable opinion of Supplier/Company any Client Business Data is not fit for the purpose for which it is used and/or disclosed by Supplier/Company and/or any Supplier/Company Group Company and/or any Supplier/Company Affiliate, then Supplier/Company must promptly inform Client and suggest appropriate changes to be made to the Client Business Data in question.

(l) Supplier/Company and each Supplier/Company Group Company and/or each Supplier/Company Affiliate undertakes not to change the format of any Client Business Data unless such change is agreed to in writing by Client or is necessary for the purposes for which Supplier/Company and/or any Supplier/Company Group Company and/or any Supplier/Company Affiliate are permitted to use the Client Business Data by Client.

(m) Where Supplier/Company or any Supplier/Company Group Company and/or any Supplier/Company Affiliate creates Client Business Data for use within Controlled Systems, the Client Business Data must be provided to Client in such format as is reasonably specified by Client.

(n) Client may identify priority areas for improving the quality of Client Business Data and may set standards, such as KPIs, relating to the quality of Client Business Data. Subject to application of the contract change process, Supplier/Company must ensure that any Client Business Data which it creates or uses, meets or continues to meet (respectively) such relevant data quality standards. Supplier/Company must also, where requested by Client, provide reasonable assistance to Client with respect to monitoring, measuring, and reviewing the quality of Client Business Data.

(o) This Exhibit I is without prejudice to any other restrictions on Supplier/Company elsewhere under this Agreement or corresponding Supplement including those relating to IP, sub-contracting and confidentiality.

(p) The Parties agree to comply with all agreed Data Use Annexes.

## **1.2 Additional IT Service requirements**

(a) Supplier/Company must ensure that Deliverables (digital or otherwise) are provided in the format reasonably requested by Client.

(b) Supplier/Company must ensure that the Services:

(i) are provided without causing loss, damage or interference to any IT Systems or Client Data;

(ii) do not cause or allow to be introduced into the IT Systems any viruses, malware, Trojan horses or other malicious code designed to:

(A) disable, damage, erase, disrupt or impair the normal operation of computer systems (including impairing software security programs residing on computer systems);

(B) assist in or enable theft, deletion or alteration of data; and/or

(C) provide unauthorised access to computer systems, software and/or data.

(c) If, as part of its provision of the Services, Supplier/Company or any Supplier/Company Personnel is permitted access to any part or parts of the IT Systems, whether directly or remotely ("Supplier/Company Access"), Supplier/Company must ensure that:

(i) if requested by Client, Supplier/Company will make available to Client and keep up to date a list of Supplier/Company Personnel who should be permitted Supplier/Company Access;

(ii) only Supplier/Company Personnel reasonably required for the proper performance of the Services are instructed by Supplier/Company to exercise such Supplier/Company Access and only in respect of those parts of the IT Systems necessary for such performance; and

(iii) Supplier/Company Personnel who conduct Supplier/Company Access comply with any specific security and access procedures and requirements applicable to those IT Systems (including the sites where they are located), as notified to Supplier/Company from time to time (as well as those procedures and requirements set out in Schedule 15 (Information Security)).

(e) Supplier/Company must not make any alteration (including updates or upgrades) to any part of an IT System without obtaining the prior written consent of Client.

### 1.3 Client Business Data analytics

(a) The following provisions apply to all access to and use of Client Business Data for the provision of Services involving analysis of Client Business Data:

(i) If an application or tool is required to derive data from Client Business Data, such tool must be subject to Client's prior review and approval;

(ii) Supplier/Company must ensure that Client Business Data is not co-mingled with any other data, save where non-Client Business Data is used to create Client Derived Data and such use is authorised by Client.

<b>Data Use Annex</b>	<i>a supplementary annex used to document a specific authorisation and/or controls relating to Unilever Business Data/Special Unilever Business Data;</i>
<b>IT Systems</b>	<i>any networks, devices, equipment, systems, applications, software or other such technical elements being used or made available by or on behalf of Unilever and/or Unilever Affiliates from time to time in connection with the Goods and/or Services;</i>
<b>Special Unilever Business Data</b>	<i>Unilever Business Data designated as "Special" by Unilever and/or any Unilever Affiliate;</i>
<b>Unilever Data/ Unilever Business Data</b>	<i>any:</i> <i>(i) data or information supplied, created, inputted or made available to the Supplier by or on behalf of Unilever and/or Unilever Affiliates;</i>

- (ii) *data or information received, collected or generated by Supplier and/or Supplier Affiliates in the course of providing Goods and/or Services under a Statement of Work;*
- (iii) *data or information received or collated from third parties for the benefit of Unilever and/or Unilever Affiliates;*
- (iv) *Unilever Derived Data; and/or*

*any record of the above data or information, including all diagrams, drawings, text, sound, videos, images or software (together with any database made up of any of these), on any media.*

***Unilever Derived  
Data***

*data or information that is derived, generated or inferred by or on behalf of Supplier and/or Supplier Affiliates in the course of providing Goods and/or Services under a Statement of Work, regardless of how it may be recorded or remembered, but excluding data or information which the Supplier creates in the normal course of business for the purposes of establishing and managing its commercial and/or legal relationship with Unilever (and/or any Unilever Affiliate).*

## **EXHIBIT D**

### **RPP and ABC**

In each case, defined terms shall have the meanings given in this Exhibit D.

At all times “you” shall refer to Supplier, and Customer/Client shall be referred to as “Genpact/Unilever”.

#### **1. Responsible Partner Policy Requirements and USQS:**

- a. You have read Unilever’s Responsible Partner Policy (“**RPP**”) as found at [www.unilever.com/responsible-partner-policy](http://www.unilever.com/responsible-partner-policy) and understand that it replaces all previous versions of the Responsible Sourcing Policy, Supplier Code or Responsible Business Partner Policy. You represent that you have your own codes of conduct and associated policies and procedures that are consistent with the requirements of the RPP. You therefore agree that you shall ensure that, by the implementation of your own codes of conduct and associated policies and procedures, you and each of your affiliated group companies each can and that you shall meet or exceed all of the requirements of the RPP, inclusive of:

- (i) Mandatory Requirements;
- (ii) related Mandatory Management Systems; and
- (iii) as they become binding under the terms of the RPP, the Future Mandatory Requirements.

These three types of requirements are each set-out in the RPP (and are individually and together “**RPP Requirements**”).

- b. You must on request by Unilever/Genpact register with the supplier assurance and compliance system, referred to as the Unilever Supplier Qualification System (“**USQS**”) or other applicable onboarding platform for downstream partners and any other non-supplier third parties, and complete any steps required to achieve compliance under such platform, including re-registering and updating information related to your organisation and (at your cost) any third-party audits as or when required by Unilever and to rectify any non-compliance identified in such audits within a timeframe stipulated by Unilever.

#### **2. ABC Requirements**

- a. Without limiting any of the RPP Requirements, you represent and undertake that:
  - i. At the date of the entering into force of the SOW, you, your directors, officers or employees have not offered, promised, given, authorized, solicited or accepted any undue pecuniary or other undue advantage of any kind (or implied that they will or might do any such thing at any time in the future) in any way connected with the Agreement and that you have taken reasonable measures to prevent subcontractors, agents or any other third parties subject to your control or determining influence, from doing so.
  - ii. At all times in connection with and throughout the course of the Agreement and thereafter, you will comply with and that you will take reasonable



measures to ensure that your subcontractors, agents or other third parties subject to your control or determining influence, will comply with Part I of the ICC Rules on Combating Corruption 2011, which is hereby incorporated by reference into the Agreement, as if written out in the Agreement in full.

- iii. No payment shall be made by you, your group affiliated companies, by subcontractors, agents or other third parties to anyone for any reason on behalf of or for the benefit of a Unilever Group company which is not properly and accurately recorded in your books and records, including the amount, purpose and recipient, all of which shall be maintained with supporting documentation.

### 3. Economic Sanctions Compliance Requirements

The “**Economic Sanctions Requirements**” shall be as follows:

- a. You represent and warrant on the date of this SOW, on the date of any invoice issued under this SOW or a related purchase order, on each date on which each shipment or delivery of products, services and/or materials is dispatched and on each date on which any invoice is settled, that you are: (1) not named on a governmental asset freezing or restricted list, including but not limited to: the United Kingdom Consolidated List of Sanctions Targets, the European Union Consolidated List of Persons, Groups, and Entities subject to EU financial sanctions and the United States Specially Designated Nationals and Blocked Persons List; (2) not organized under the laws of, or providing services or goods from, a jurisdiction subject to comprehensive sanctions (currently; Cuba, Iran, North Korea, Syria, the Crimea region, the Donetsk People's Republic, and the Luhansk People's Republic); and (3) not controlled, or owned (directly or indirectly) 50% or more in the aggregate, by one or more of any of the foregoing (together, “**Restricted Party**”), and (4) has not breached any Trade Control Laws.
- b. You agree to comply with all applicable Trade Control Laws, including those relating to the direct or indirect use, diversion, trade, export or re-export of products, services and/or materials (including any regulations prohibiting drugs and weapons manufacture). “**Trade Control Laws**” means all applicable trade or economic sanctions or embargoes, controls on the imports, export, re-export, use, sale, transfer, trade, or otherwise disposal of goods, services or technology, anti-boycott legislation or similar laws or regulations, rules, restrictions, licenses, orders or requirements in force from time to time, or applicable to the use of a currency or a method or route of payment, as the same may be applicable directly or indirectly to you or your value chain. Such laws shall be deemed always to include such laws or regulations in force at the time within the European Union, the United Kingdom, the United States of America. Without limiting the foregoing, in connection with your performance of the contract documents, you shall: (1) not transact (directly or indirectly) with a Restricted Party; and (2) not source (directly or indirectly) any goods or services from a jurisdiction subject to comprehensive sanctions (currently Cuba, Iran, North Korea, Syria, the Crimea region, the Donetsk People's Republic, and the Luhansk People's Republic). For territories regarded by Unilever/Genpact as medium or higher risk territories, as the same are listed from time to time on <https://www.unilever.com/suppliers/terms-and-conditions/>, you agree to promptly disclose for medium or higher-risk territories all information requested reasonably by Unilever/Genpact in order to verify your compliance with this paragraph along the entire value chain, so as to verify that no breach of Trade Control Laws has occurred or is occurring.

- c. Without limiting other requirements, you must (at your own cost) maintain comprehensive, accurate and reliable records of all activities undertaken to comply with the foregoing Economic Sanctions Requirements, evidencing in particular your screening of counterparties and their paying and remitting banks at each stage of the value chain for the involvement of Restricted Parties. You shall promptly alert Unilever to any known potential or apparent violations of any of the Economic Sanctions Requirements and cooperate in any investigation or remedial action.

#### **4. Breach of RPP, ABC, or Economic Sanctions Requirements**

- a. You shall promptly alert Unilever/Genpact:
  - i. regarding any known potential or apparent violations of any of the RPP, ABC, or Economic Sanctions Requirements, and cooperate in any investigation thereof and remedial action;
  - ii. if a public official (or a person who has been a public official within the previous two years) becomes a significant shareholder (>25% shareholding), a member of the senior management team, member of the Board of Director, or key individual in your company group or in an associated person, including subcontractors who will be responsible for the provision of goods / services to Unilever; and
  - iii. if, at any point, you are unable to meet or comply with one or more of the requirements of the RPP, ABC or Economic Sanctions Requirements.
- b. If any member of your company group fails to meet or comply with one or more of the requirements of the RPP, ABC or Economic Sanctions Requirements, then where Unilever considers that such a breach can be remediated, you shall take all further steps as reasonably stipulated by Unilever/Genpact to remedy the breach, including the implementation of adequate procedures so that no such breach will occur again.
- c. If Unilever has a reasonable basis to believe that a member of your company group or any subcontractor of the same is not in compliance with or does not meet one or more of the requirements of the RPP, ABC or Economic Sanctions Requirements, or where concerns arising out of a confirmed breach are material and the breach cannot be or is not remedied in accordance with the requirements set out above, then Unilever shall have the right, exercisable at Unilever's /Genpact's sole discretion:
  - i. to suspend by notice, without Genpact or Unilever Group company liability arising, immediately any and all services and payments under any purchase order and/or this SOW; and/or
  - ii. to terminate without Genpact /Unilever Group company liability arising, immediately on notice any purchase order and/or this SOW.
- d. Without limiting the rights under this clause, any breach of the RPP, ABC, or Economic Sanctions Requirements shall be rectified by you at your cost within the timeframe stipulated by Unilever/Genpact and shall be prevented from re-occurrence.

- e. You agree to indemnify and hold each Unilever/Genpact Group company and their officers harmless against all costs, claims, damages and expenses which Unilever Group companies or their contractors may be liable for or suffer, including fines and costs of defence, and settlements payable to an entity or person, due to any alleged or actual failure by you or your company group to comply with or failure to meet one or more of the RPP, ABC or Economic Sanctions Requirements.

#### **5. Update of RPP, ABC, or Economic Sanctions Requirements**

Unilever/Genpact may from time to time amend and update the RPP, ABC and Economic Sanctions Requirements, and shall inform you of such amendments and updates, at no cost to Unilever. If you are not then able to meet one or more of the requirements imposed by the amendments or updates, then you must contact Unilever/Genpact within 8-weeks of Unilever informing of such amendment or update in order to agree with Unilever an implementation plan and schedule for such requirements. Where any failure to meet or failure to comply with RPP, ABC, and Economic Sanctions Requirements leads to a breach of applicable law by you, you must inform Unilever/Genpact and comply with the requirement and the applicable law immediately.

**EXHIBIT E**  
**SERVICE LEVELS**

**13. SCOPE & PURPOSE**

This schedule sets out:

- (a) the Service Levels which the Service Provider is required to achieve when delivering the Services;
- (b) the KPIs which will be additional indicators of the Service Provider's performance of the Services;
- (c) the Service Provider's responsibilities for developing and implementing remedial plans in the event of a Service Level Miss; and
- (d) the method by which the Service Provider's performance of the Services will be monitored.

**2. PERFORMANCE STANDARDS AND SERVICE LEVELS**

**2.1 General:**

- (a) For Service Levels that do not have historical data, then for six (6) months post Go Live of the Services in the relevant wave, the Service Provider shall baseline the Service Levels in respect of that Service. Post the baseline activities the Parties shall agree on the Service Levels for those Services.
- (b) For Service Levels that have historical data, then upon Go Live of the Services in the relevant wave, the Service Provider shall achieve or exceed those Service Levels in respect of that Service. Ramp-up plan will be mutually agreed between both the parties for addition of any scope or region.
- (c) The Service Provider shall perform each Service under this SOW:
  - (i) without prejudice to the other provisions of this section with promptness, skill, care and diligence, in a professional manner and in accordance with good industry practice and Applicable Law;
  - (ii) without prejudice to the other provisions of this section using efficiently the resources or services necessary to provide the Services; and
  - (iii) without prejudice to the other provisions of this section using individuals who:
    - (A) are appropriately experienced, qualified and trained;
    - (B) are familiar with the requirements set out in this SOW; and
    - (C) shall perform the Services with all reasonable skill, care and diligence.

**2.2 Service Credits**

- (a) The Service Provider acknowledges that its failure to meet a Service Level by region, may have a commercial and operational impact on Genpact.
- (b) If the Service Provider fails to meet the Expected Level of:
  - (i) Any particular service level for three consecutive measurement periods the provisions of Service Credits shall apply.
  - (ii) In the event that service credit applies pursuant to 2.2 (b) (i) above, the service provider shall be liable to an amount equivalent to twelve per cent (12%) of the charges for the month immediately following the three consecutive measurement period
- (c) For any Service Credit resulting from a Minimum Service Level Miss, the Service Provider has the right to earn back one hundred percent (100%) of the applicable Service Credit ("Earnback Credit") to the extent it was paid to Genpact, if:
  - (i) during the 6-month period commencing in the month after which the Service Provider failed to meet the Minimum Service Level for the relevant Service Level Miss ("Earnback Period"), the Service Provider's actual performance on average exceeds the Expected Service Level for that service; and
  - (ii) provided that there is no further failure to meet the Minimum Service Level in that 12-month period. Any such failure would cause the Earnback Period to end and then be re-started in the following month.
- (d) Within ten (10) Business Days of the expiry of the Earnback Period, the Service Provider shall provide Genpact with a report setting out the Service Provider's performance for the relevant service over the Earnback Period and the amount of Earnback Credits (if any) due to the Service Provider. Provided that the Service Provider's report has demonstrated to Genpact's reasonable satisfaction that the Service Provider's overall performance for the relevant service in the Earnback Period entitles the Service Provider to an Earnback Credit, an Earnback Credit will be added to the next monthly invoice.

### 2.3 Periodic Reviews

- (a) Genpact and the Service Provider shall review the Service Levels no later than six months after the completion of Transition, and thereafter annually.
- (b) As part of this review, the Parties may agree adjustments to the Service Levels as appropriate, including adjustments so as to reflect improved performance capabilities associated with advances in the technology and methods used to perform the Services, as well as to accommodate improvements in Services delivery brought about by the fulfilment by the Service Provider of its obligations.
- (c) Any adjustments pursuant to Section 2.3 (b) shall be documented as Changes using the Change Control Procedure. The Parties expect and understand that the Service Levels may be varied over time; however, to the extent that either Party proposes a reduction in Service Levels, such reduction shall only be proposed on the basis that there is a corresponding reduction in the Charges to account for the reduced level of Service provided.

## 2.4 Measurement and Reporting

The Service Provider shall measure and report its performance against the Service Levels at the level of frequency, and in accordance with the reporting requirements jointly agreed. The Service Provider shall provide Genpact with information and access to those measurement and monitoring tools and procedures and on request, to enable Genpact to verify that they measure the Service Provider's performance accurately.

## 2.5 Persistent failure to achieve Service Levels

If the Service Provider breaches the same Minimum Service Level in four (4) Measurement Periods during any rolling six (6) Measurement Periods duration, then at Genpact's option, Genpact may, upon notice to the Service Provider, terminate this SOW.

The Service Provider will provide each Service to a standard which meets the Expected Service Level to be jointly agreed between Genpact and the Service Provider.

## 2.6 Each Service Level Table, agreed before the commencement date, should set out, in respect of each Service:

- (a) a description of the Service being measured;
- (b) the measurement required;
- (c) the Measurement Period;
- (d) Measurement methodology;
- (e) Sampling methodology;
- (f) the required Service Levels, being:
  - (i) a "**Minimum Level**" or "**Minimum Service Level**" – where a failure to meet or exceed this level would be of such a fundamental nature that Genpact would be entitled at its sole discretion to immediately exercise its Step-in Rights to take control of the relevant service;
  - (ii) an "**Expected Level**" or "**Expected Service Level**" - where a failure to meet or exceed this level would constitute a Service Level Miss; and
- (g) whether a service is designated as a KPI.

## 3. SERVICE LEVEL MISSES

### 3.1 Without prejudice to any other right or remedy of Genpact, following the occurrence of a Service Level Miss, the Service Provider will:

- (a) promptly notify Genpact of such Service Level Miss;
- (b) investigate, assemble and preserve pertinent information with respect to, and report as part of the Service Level Management Information on the cause(s) of, the relevant Service Level Miss;

- (c) process any Service item backlog through suitable workarounds, ensuring that all necessary expertise and resources are committed to address the underlying problem and otherwise minimise the impact of the Service Level Miss; and
  - (d) take appropriate preventative measures to seek to minimise the likelihood that the relevant Service Level Miss will recur.
- 3.2 The Service Provider shall not knowingly, deliberately or recklessly act in such a way as to prejudice its ability to meet any particular Service Level in order to meet another Service Level.

#### 4. **REMEDIAL PLANS**

- 4.1 Without prejudice to any other right or remedy of Genpact, following the occurrence of a Service Level Miss, the Service Provider shall perform a root cause analysis of the same and provide a detailed remedial plan to Genpact within five (5) Business Days after the occurrence of the Service Level Miss, setting out the steps which the Service Provider intends to take to ensure that the Service Level Miss is remedied, to minimise the impact of the failure, and to minimise the likelihood that the relevant Service Level Miss will recur. If the remedial plan is acceptable to Genpact (acting reasonably), then the Service Provider shall implement the provisions of the remedial plan without delay and at no cost to Genpact, only if the occurrence was due to reasons attributable to the Service Provider.
- 4.2 During the execution of any remedial plan, the Service Provider shall continually monitor the work undertaken and report the result to, and review the results with, Genpact.
- 4.3 If the Service Provider fails to implement a remedial plan for failure to achieve a Minimum Service Level in accordance with Section 4 of this schedule which is acceptable to Genpact within the timescales set out therein, and following escalation of the issue pursuant to the governance procedures then Genpact may (but shall not be obliged to) exercise its rights of step-in ("**Step-in Rights**") to remedy such failure.
- (i) The exercise of Step-in Rights by Genpact, and the responsibilities of the resources used in step-in shall be limited to the remediation of failed Service Levels as set out in this Section.
  - (ii) Genpact shall implement its Step-in Rights by the use of Genpact associates on Genpact premises or on Service Provider premises.
  - (iii) Upon successful completion of the remediation, as defined by achievement of the Minimum Service Level for the services being remediated, and in any event after not more than 45 days, the resources used to execute the Step-in Rights shall step out and responsibility for delivery of the affected Services shall be resumed by the Service Provider.

#### 5. **CONTINUOUS IMPROVEMENT OF SERVICE LEVELS**

The Parties acknowledge that a key requirement of Genpact in the procurement of the Services from the Service Provider is to improve the standard to which the Services are provided over the course of the Term to achieve the Target Service Levels. Accordingly, save as otherwise agreed by the Parties pursuant to the Change Control Procedure, the Expected Level and Minimum Level of each Service Level or KPI shall be reviewed annually by the Parties, based

on performance during the previous 12 months and the business requirements from Genpact, and they may be altered by mutual agreement of the Parties.

## 6. **MEASUREMENT AND REPORTING**

### 6.1 **General**

- (a) To the extent not agreed prior to the Go Live date, the format and content of any Service Level Management Information shall be agreed between the Parties (acting reasonably and promptly) during Transition. To facilitate such process, the Service Provider shall provide sample, anonymised, standard reports which it produces for other customers to Genpact for Genpact's review during the Transition Period.
- (b) Where the Service Level Management Information indicates a reduced level of performance of any Service (as compared to the previous month), the Service Provider shall perform root cause analysis and make appropriate recommendations and comments relating to the relevant Service (as part of the relevant Service Level Management Information).
- (c) Genpact reserves the right independently to measure the Service Provider's performance of this SOW. In the event of any discrepancy between the measurements undertaken by the Service Provider and those undertaken by Genpact, the Parties will discuss such discrepancy at the next meeting of the monthly Service Management Board.

### 6.2 **Frequency**

The Service Provider shall provide Genpact with the Service Level Management Information no later than Five (5) Business Days after the end of each reporting period, unless otherwise agreed in writing between the Parties (acting reasonably), and Genpact shall be entitled to raise any queries it may have in respect of the Service Level Management Information ahead of the relevant meeting.

### 6.3 **Measuring Performance and Reporting of Service Credits**

The Service Provider will ensure that the Service Level Management Information provided pursuant to this agreement demonstrates that the Service Provider's performance of the Services meets or exceeds the Expected Service Level for each Service Level or otherwise that a Service Level Miss has occurred.

## 7. **Service Level Relief Events**

Degradations or failure of performance shall not constitute a failure by Service Provider to comply with the Service Levels to the extent that any such failure is attributable to any one or more of the following causes ("**Service Level Relief Events**"):



- (a) the acts or omissions of Genpact, including failure to perform Genpact Obligations;
- (b) Service or resource reductions requested or approved by Genpact;
- (a) a Force Majeure Event; or
- (c) downtime agreed by both Parties for the purposes of emergency or scheduled maintenance
- (d) Unscheduled / unprojected volume surges over and above the agreed exception levels.

8. The SLAs that will apply to this SOW are tabulated as follows:

**EXHIBIT F**  
**BUSINESS CONTINUITY MANAGEMENT PLAN**

**BUSINESS CONTINUITY MANAGEMENT  
(BCM)**



**NextWealth Entrepreneurs Pvt. Ltd.**  
Indique Celestia  
4th Floor, Site No. 19 & 20,  
Koramangala 1A Block,  
Bengaluru, Karnataka 560034

**Confidential**

This document contains confidential information of Next Wealth. In consideration of receipt of this document, unless governed by other contractual agreement between Next Wealth and the recipient, the recipient agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible and authorized to use its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from Next Wealth, or becomes publicly known through no fault of recipient, or is received without obligation of confidentiality from a third party.

**Business Continuity Management  
V3.0****Document control Information**

Issue Version (Release)	Summary of changes	Author	Approved By	Effective Date
1	Baseline	Prabhu SV	Demoderan S	08-Aug-2023
2	Changes to facilities included in the table	Prabhu SV	Demoderan S	20-Aug-2023
3	Rephrase the Business Impact Analysis score section for better understanding	Prabhu SV	Demoderan S	21-Sep-2023

## Business Continuity Management (BCM)

BCM Primary Owner: Center Head (Damodaran Selvaraj)

BCM Secondary Owner: Operations Head (Prabhu S V)

BCM / NWERT Team Members:

Sl.No.	Name	Function / Dept	Contact
1	Mythily Ramesh	NW HO	9845058964
2	Mahesh Tallam	NW HO	9901888800
3	Jayanth Samprathi	NW HO	9845455372
4	Jagadisha S H	NW HO	9591907097
5	Deepa Haridas	NW HO	9845658922
6	Damodaran Selvaraj	Center Head	9489900060
7	Priya Thanikachallam	Transition SPOC	9845472705
8	Prabhu S V	Operations Head	9094311223
9	Vinothkumar S	HR, Training & Admin	9489900480
10	Sunilbabu S	Risk & Compliance	9489900051
11	Hariharan A	System Administration	9489900054

**Business Continuity Management  
V3.0**

**Business Impact Analysis Scores**

The following number scores have been established to provide firm tangible and intangible exposure categories for cross-cluster comparison.

Cumulative Loss Ranges (Tangible) per day if the process doesn't function (Below are the tentative loss and will be changed/modified based on the project study).

Note: The loss mentioned below is just to evaluate the impact and the related actions to be taken accordingly and not to specify the actual loss. This is an approximate estimated impact of the idle time. It helps in highlighting the criticality of service outage. And helps to decide the right methodology and time frame for the chosen BCP. (Detailed template will be filled once the SOW is signed)

Score	Loss Range
0	None
1	< Rs.1,000
2	≥ Rs.1,000 < Rs.5,000
3	≥ Rs.5,000 < Rs.10,000
4	≥ Rs.10,000 < Rs.25,000
5	≥ Rs.25,000 < Rs.50,000
6	≥ Rs.50,000 < Rs.100,000
7	≥ Rs.100,000 < Rs.150,000
8	≥ Rs.150,000 < Rs.250,000
9	≥ Rs.250,000 < Rs.500,000
10	≥ Rs.500,000

**Definitions of Intangibles:**

Impact Category	Definition
Loss of Revenue	Loss of income received from selling goods or services
Additional Expenses	Temporary staffing, overtime, equipment, services
Regulatory and Legal	Fines, penalties, compliance issues, contractual obligations, financial liabilities
Customer Service	Termination or reduction of service level (internal or external), live operators vs. automated response
Goodwill	Public image, shareholder relations, market share

Score	Effect
0	None
2	Minimal
4	Moderate
6	Moderately Heavy
8	Heavy
10	Severe

### Business Impact Analysis – Invoice Processing Salem Operations

Business Unit/Department Name: NW Operations  
 Business Process Name: Genpact Salem Operations  
 Business Function Description: Invoice Processing

1. Committed "Service window": 16 x 5

9 x 6	10 x 3	16 x 5	24 x 7
-------	--------	--------	--------

2. Using the Impact categories to classify the type of loss incurred and the Loss ranges (0 through 10) specify your actual amount of exposure during the disaster below:

Impact Category	Impact Score
Cumulative Loss Ranges (Tangible) per day (0 to 10)	7 (Approx. evaluation. Will re-evaluated as per the commercials in SOW)
Additional expenses (per day)	3 (Approx. evaluation. Will re-evaluated as per the commercials in SOW)
Regulatory and legal (per day)	3 (Approx. evaluation. Will re-evaluated as per the commercials in SOW)
Goodwill Overall	8 (Approx. evaluation. Will re-evaluated as per the commercials in SOW)

3. Is this function dependent on any technology (hardware or software):  
 Yes

Technology details	Contact person and contact details
Application	<<To be provided by Client Authorities>>
Connectivity	<<To be provided by Client Authorities>>
RTO & RPO	<<To be provided by Client Authorities>>
Internet, Email, DNS, AD	Dinakaran K – Mahendra Next Wealth IT India Pvt. Ltd. 96884 86600
Network Security	Hariharan A – Mahendra Next Wealth IT India Pvt. Ltd. 9489900054 <<Also the Counterpart in Clientside, to be provided by Client Authorities>>

## Outside services provider details:

Outside Services	Contact person and contact details
INTERNET	BSNL – Mohanraj - 9486103062 Tata – 18002661515 if not resolved in 4 hrs. Raghavendra Kumar R – 9282109475 Readylink – CSR No. 9894700011 Airtel – Helpdesk No. 1800102001
TNEB	Ravi – 8883210784

## BCM Plan - Continuity of IT &amp; Operations

In the event of Business Continuity situation due to any legal restrictions or any natural disturbances and Civil Authorities restricting travel of employees / Mass power cut / Technology issues / confining the employees to their homes in a geographic area, resulting in employee's inability to reach the delivery center premises by any modes of transport.

The following steps would be undertaken specific to Invoice Processing Clients specified operations as a measure to maintain the delivery of services

## 1. Hardware

- 1.1. Personal Computer or Laptops: NextWealth would provision a hardware that would be a personal computer at identified employees' residence
- 1.2. The personal computer would be hardened as per standard guidelines followed and kept ready
- 1.3. The hardware would include the computer, the display screen, the keyboard and a mouse

## 2. Network Connectivity

- 2.1. Each agent home shall be connected by the best possible mode of connectivity in the below sequence of priorities and subject to its availability
  - Broadband - DSL
  - Internet Dongle
  - Hotspot from Employees' Cell Phone
- 2.2. NextWealth has a list of best available modes of connecting to Internet at Employees' residence premises, it would determine the best possible mode

### **3. Network Security**

- 3.1. Each agent once connected to the Internet, will use a VPN client to connect with the delivery center securely by entering the needed username / password and other security credentials
- 3.2. VPN client would be connecting with the Central Firewall and Access policies shall be preconfigured to ensure each Agent can access his / her specific applications only
- 3.3. A firewall policy shall be enabled for agent, allowing them to use specific port numbers of the applications

### **4. Client Application Access**

- 4.1. NextWealth shall provide a list of identified agents who would be accessing the network and the applications remotely
- 4.2. Agents shall be allowed to access pre-authorized (existing) applications only after connecting via VPN
- 4.3. The same credentials that are currently prevalent shall be used for the purpose
- 4.4. Genpact, to mention the BCP for the client application

### **5. Overall IT Testing**

- 5.1. NextWealth shall be performing a basic test and keeping the IT and operational ecosystem ready for enabling the agents to remotely work from home
- 5.2. NextWealth shall provide a test report from an agent's residence after the due steps have been completed
- 5.3.

### **6. BCP – Testing Plan & Learnings**

- 6.1. NextWealth will come up with quarterly BCP testing plan
- 6.2. We will execute the test plans for various test scenarios at center level
- 6.3. The feedback will be given after the BCP to take the learnings forward

### **7. Employee identification**

- 7.1. A list of employees will be prepared in advance with their residence address, alternate contact number and available infrastructure on the spot
- 7.2. They will be informed of their roles in case of a disaster and their responsibility
- 7.3. They will be trained to work with this set up

### **8. Communication plan**

- 8.1. All stake holders will be informed of the disaster in all situation
- 8.2. The type of BCP, will be invoked will be based on the discussion and decision with the management
- 8.3. Immediately everyone must start performing their identified work

### **9. Roles & Responsibilities in brief**



**Business Continuity Management  
V3.0**


- 9.1. HR & Training will document all awareness to be given to agents and give required training. Operations will work with HR for this.
- 9.2. Client will identify the work that needs to be executed during disaster, prioritized the work during the disaster, and communicate the same to the NextWealth operations team. Operations will have list of all agents who will work from home and inform them when the disaster is declared. Will track their performance and ensure control.
- 9.3. During the BCP situation, SLA will be tracked and there will be accepted deviation on the SLA and TAT as and when decided based on the level of impact.
- 9.4. Admin will do all required shifting and transport of infra as well the agents as required.

**10. Facilities for People:**

Current Mode of Work	Facilities
Employees in WFO	Dedicated desktops and required infrastructure will be shifted to every employee's home within 24 Hrs to 48 Hrs
Employees in WFH	Can look at either an already working broadband or we can look at started working with a temporary mobile connection.
Alternate for WFH/WFO	Employees are recommended to work from nearby centers of NextWealth with the Client's approval. This option will involve cost and decided based on mutual consent.

**11. Key Notes**

- 11.1. Movement of desktops to agent houses is dependent on the external situation and safety of employees.
- 11.2. There would be additional commercials towards additional hardware (personal computer or laptops) being deployed in the agent's residence along with the charges for Internet Access.
- 11.3. There may be no availability of UPS (Uninterrupted Power Supply) at the Agent's residence.
- 11.4. As internet access is disparate in the quality of bandwidth available at the agent's residence location, NextWealth cannot assure a minimum standard bandwidth availability and there could be an impact on the production.
- 11.5. During the situation of Business Continuity, and especially with the agents working from home, NextWealth will not be in a position to comply with the guidelines completely as per ISO 27001. The compliance levels would be on a best-effort basis and with basic controls in place.
- 11.6. Operational control and monitoring will be done daily but remotely. Infrastructure and remote working may impact the efficiency, productivity and utilization.

**12. Network Block Diagram****13. Timelines & Schedule: (We need to sync it up with Options under "Solutions Options")****Post declaration of outage/BCP:**

- Restoration of 50% in 24 hours.
- Restoration of 100% in 48 hours.

Parameters like; the situation on the ground, availability of resources and safety of resources, expected outage period etc., will be considered and the possibility of altering the restoration % will be considered post-mutual discussion.

**14. BCP for People Factor**

- Criteria 1 - Complete lockdown:
  - Keep an updated agent list with staying location address and phone number, this report will be updated every 3 months.
  - Employees who requested for Hostel Stay will be provided
  - Evaluate the system movement method like cab, own vehicle
  - Plan for connectivity method – Devices (Dongle, Broad band, Broad band Fibre net connection, Mobile phones tethering) Data recharges for Dongle and mobile reimbursement of broadband bills)
  - Attendance and availability check as per that work needs to be allocated
  - Tracking the power cut helps employees to log in early which helps to complete their task on time

- **Criteria 2 - Partial lockdown:-**

- Keep an updated agent list with staying location address and phone number, this report will be updated every 3 months.
- Employees who requested for Hostel Stay will be provided
- Evaluate the system movement method like cab, own vehicle
- Plan for connectivity method – Devices (Dongle, Broad band, Broad band Fibre net connection, Mobile phones tethering) Data recharges for Dongle and mobile reimbursement of broadband bills)
- Attendance and availability check as per that work needs to be allocated
- Tracking the power cut that helps employees to login early which helps to complete their task on time