

## SCHEDULE C — DATA SHARING & PROCESSING AGREEMENT (DPA)

**⚠️ DRAFT — must be reviewed by a PH data-privacy practitioner. Not legal advice.** Drafted to the Data Privacy Act of 2012 (RA 10173), its IRR, and National Privacy Commission (NPC) issuances. [brackets] = to confirm. Forms part of the MOA.

### 1. Roles

1.1 For **Customer Personal Data** collected via the Marketplace, **Philstar is the Personal Information Controller (PIC)** and **bXTRA is the Personal Information Processor (PIP)** processing on Philstar's documented instructions **[to confirm — could be joint-PIC for certain processing]**. 1.2 For **rider/operational data** that bXTRA collects to run delivery, **bXTRA acts as PIC** for its own workforce/fleet data. 1.3 Each Party is independently accountable for its own compliance, registration with the NPC (if required), and appointment of a **Data Protection Officer (DPO)**.

### 2. Subject matter & purpose

bXTRA Processes Personal Data **only** to provide the Services (order fulfilment, delivery, payouts, support, fraud prevention, and reporting) and for no unrelated purpose. No selling of personal data.

### 3. Categories of data & data subjects

DATA SUBJECTS	PERSONAL DATA (ILLUSTRATIVE)
Customers	name, contact number, delivery address, order details
Seller contacts	name, business, contact details
Riders (bXTRA PIC)	name, contact, location during delivery, payout details

Collect only what is necessary (data minimisation). **No sensitive personal information** is required for the core flow; if any is introduced, the Parties shall first agree safeguards and lawful basis.

### 4. Lawful basis & consent

Processing relies on **[contract performance / legitimate interest / consent]** as applicable. Philstar (PIC) is responsible for the privacy notice and obtaining any required **consent** from Customers at the point of collection on the Marketplace.

### 5. Obligations of bXTRA (PIP)

bXTRA shall: (a) Process only on Philstar's documented instructions; (b) ensure persons authorised to Process are bound by confidentiality; (c) implement the security measures in Section 8; (d) assist Philstar with data-subject requests and breach/DPIA obligations; (e) not engage sub-processors except per Section 6; (f) on termination, **delete or return** Personal Data per Section 9; (g) make available information to demonstrate compliance and allow reasonable audits (Section 10).

### 6. Sub-processors

6.1 bXTRA may use sub-processors (e.g., hosting/cloud, SMS/notification, payment, mapping) **listed in Annex C-1**, with **[general/specific]** authorisation. 6.2 bXTRA shall impose equivalent data-protection obligations on each sub-processor and remain liable for their acts/omissions. Philstar will be notified of new sub-processors with **[15] days** to object.

### 7. Data-subject rights

bXTRA shall, within **[5] business days**, assist Philstar in responding to data-subject requests (access, correction, objection, erasure/blocking, data portability, and to be informed) under RA 10173.

### 8. Security measures (organisational, physical, technical)

- Access controls, least-privilege, unique credentials, and **[MFA]** for admin consoles.

- Encryption **in transit (TLS)**; encryption at rest for stored Personal Data **[where applicable]**.
- Tokenised/role-based access in the maker & ops consoles (a Seller sees only its own orders).
- Logging, monitoring, regular backups, and vulnerability management.
- Staff confidentiality undertakings and privacy training.
- *(Current build note: demo consoles use a shared token — production will use per-role/per-seller authentication before any real Personal Data is processed.)*

---

## 9. Retention & deletion

Personal Data retained only as long as necessary for the Services or as required by law, then securely deleted/anonymised. On termination, bXTRA returns and/or deletes Personal Data within **[30] days**, certifying deletion, save for legally-required retention.

---

## 10. Breach notification

10.1 bXTRA shall notify Philstar **without undue delay and within [24–48] hours** of becoming aware of a **personal data breach**, with available details. 10.2 The Parties shall cooperate so the PIC can meet the NPC/affected-data-subject notification obligation (generally **within 72 hours** for notifiable breaches under RA 10173/NPC rules).

---

## 11. Cross-border transfer

If Personal Data is Processed or stored **outside the Philippines** (e.g., cloud regions), bXTRA shall ensure a comparable level of protection and accountability consistent with RA 10173. **[Confirm hosting region(s).]**

---

## 12. Audit

Philstar may, on reasonable notice and **[once per year / on a breach]**, audit bXTRA's compliance (or accept an independent report/certification), subject to confidentiality and not unduly disrupting operations.

---

## 13. Liability & precedence

This DPA supplements the MOA. For data-protection matters, this DPA controls in case of conflict. Statutory liability under RA 10173 is not limited by the MOA's liability cap.

---

### Annex C-1 — Sub-processors (to confirm)

SUB-PROCESSOR	PURPOSE	LOCATION
Cloudflare (Pages/Workers/KV)	hosting, edge, order/lead store	<b>[global edge]</b>
<b>[SMS / notifications provider]</b>	order updates	<b>[ ]</b>
<b>[payment provider]</b>	checkout/settlement	<b>[ ]</b>
<b>[maps/geocoding]</b>	delivery routing	<b>[ ]</b>