ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
(Data Processing Agreement)

ข้อตกลงฉบับนี้ ("ข้อตกลงนี้" (DPA)) เป็นส่วนหนึ่งของสัญญาหลักการให้บริการ (Master Services Agreement) ("สัญญาหลัก") ระหว่างผู้รับบริการตามที่ระบุในใบสั่งซื้อบริการ (Order Form) ("ผู้รับบริการ" (Customer)) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) กับ **บริษัท ศาลาแดง จำกัด** ("ผู้ให้บริการ" (Service Provider)) ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ข้อตกลงนี้ใช้กับใบสั่งซื้อบริการทุกฉบับที่อ้างถึงข้อตกลงนี้ และคู่สัญญาตกลงตามข้อตกลงนี้โดยการลงนามในใบสั่งซื้อบริการนั้น (ข้อ 12.3) คำที่นิยามไว้ในสัญญาหลักมีความหมายเดียวกันในข้อตกลงนี้ คำว่า "ข้อมูลส่วนบุคคล" "เจ้าของข้อมูลส่วนบุคคล" "ผู้ควบคุมข้อมูลส่วนบุคคล" "ผู้ประมวลผลข้อมูลส่วนบุคคล" และคำที่เกี่ยวข้อง มีความหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ("พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล" (PDPA)) ข้อตกลงนี้ใช้บังคับในเวอร์ชันที่ระบุในใบสั่งซื้อบริการ ผู้ให้บริการเผยแพร่ข้อตกลงนี้ที่ www.sala-daeng.com/agreements ตามเลขที่และเวอร์ชันของเอกสาร

ข้อ 1 บทบาทและขอบเขต

1.1 ในการให้บริการ ผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลในข้อมูลของผู้รับบริการ (Customer Data) ในนามของผู้รับบริการ ผู้รับบริการเป็นผู้ควบคุมข้อมูลส่วนบุคคล และผู้ให้บริการเป็นผู้ประมวลผลข้อมูลส่วนบุคคลของข้อมูลดังกล่าว

1.2 ข้อตกลงนี้ใช้กับการประมวลผลข้อมูลส่วนบุคคลทั้งหมดที่ผู้ให้บริการดำเนินการในนามของผู้รับบริการภายใต้เอกสารสัญญาทุกฉบับ ในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ข้อตกลงนี้มีผลเหนือเอกสารสัญญาอื่นตามสัญญาหลัก ข้อ 2 และข้อ 11

1.3 ผู้รับบริการรับรองว่าตนมีฐานทางกฎหมายในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ส่งให้ผู้ให้บริการประมวลผล และได้แจ้งเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

1.4 **ผู้เยาว์** หากใบสั่งซื้อบริการระบุว่าเจ้าของข้อมูลส่วนบุคคลรวมถึงผู้เยาว์ เช่น นักเรียน ผู้รับบริการรับรองว่าตนได้รับความยินยอมใด ๆ ที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดสำหรับข้อมูลส่วนบุคคลของผู้เยาว์ รวมถึงความยินยอมของผู้ใช้อำนาจปกครองในกรณีที่กฎหมายกำหนด ทั้งนี้สอดคล้องกับสัญญาหลัก ข้อ 11.2

1.5 **บริษัทในเครือที่ได้รับอนุญาต** ผู้รับบริการให้คำสั่งตามข้อตกลงนี้ในนามของตนเองและในนามของบริษัทในเครือที่ได้รับอนุญาต (Permitted Affiliates) และรับรองว่าตนมีอำนาจกระทำการดังกล่าว ในกรณีที่บริษัทในเครือที่ได้รับอนุญาตเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ให้บริการประมวลผลข้อมูลนั้นในนามของบริษัทในเครือนั้น และผู้รับบริการเป็นผู้ใช้สิทธิของบริษัทในเครือนั้นตามข้อตกลงนี้

1.6 **ข้อมูลส่วนบุคคลอ่อนไหว** ผู้ให้บริการไม่ประมวลผลข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลสุขภาพ ศาสนา หรือข้อมูลชีวภาพ เว้นแต่ใบสั่งซื้อบริการจะระบุไว้

ข้อ 2 รายละเอียดการประมวลผล

2.1 เอกสารแนบ DPA-1 กำหนดรายละเอียดมาตรฐานของการประมวลผลสำหรับลักษณะการประมวลผลแต่ละแบบตามข้อ 2.2 ส่วนการประมวลผลข้อมูลส่วนบุคคลในใบสั่งซื้อบริการระบุว่าลักษณะใดใช้กับผู้รับบริการ และรายการเพิ่มเติม เช่น บริษัทในเครือที่ได้รับอนุญาต เจ้าของข้อมูลส่วนบุคคลหรือประเภทข้อมูลส่วนบุคคลเพิ่มเติม ผู้เยาว์ ข้อมูลส่วนบุคคลอ่อนไหว และการยืนยันตัวตน รายการเพิ่มเติมดังกล่าว และรายละเอียดการประมวลผลใน SOW (ถ้ามี) ให้ถือเป็นส่วนหนึ่งของเอกสารแนบ DPA-1 สำหรับผู้รับบริการรายนั้น

2.2 ผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลในสองลักษณะ

(ก) **บริการที่ผู้ให้บริการโฮสต์** (Hosted Services) ผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ของตน โดยใช้ผู้ประมวลผลช่วงตามรายชื่อผู้ประมวลผลช่วง (ข้อ 6.1) ตามที่คำอธิบายบริการกำหนด

(ข) **สภาพแวดล้อมของผู้รับบริการ** (Customer Environment) สำหรับซอฟต์แวร์ที่ติดตั้งในสภาพแวดล้อมของผู้รับบริการ (Customer-Hosted Software) บริการติดตั้งระบบ บริการบำรุงรักษา และการสนับสนุน บุคลากรของผู้ให้บริการเข้าถึงสภาพแวดล้อมของผู้รับบริการจากระยะไกลหรือ ณ สถานที่ของผู้รับบริการ ข้อมูลส่วนบุคคลคงอยู่ในระบบของผู้รับบริการ ผู้ให้บริการนำข้อมูลบางส่วน (extract) ออกจากสภาพแวดล้อมของผู้รับบริการเฉพาะเพื่อการโอนย้ายข้อมูล การทดสอบ และรายการแจ้งปัญหา เก็บไว้เฉพาะในระบบของตนที่อยู่ในรายชื่อผู้ประมวลผลช่วง และลบตามข้อ 10.3

ข้อ 3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ตามมาตรา 40 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการจะ

3.1 ประมวลผลข้อมูลส่วนบุคคลเฉพาะตามคำสั่งเป็นลายลักษณ์อักษรของผู้รับบริการ ได้แก่ เอกสารสัญญาและคำสั่งผ่านช่องทางที่ตกลงกัน เว้นแต่กฎหมายไทยกำหนดเป็นอย่างอื่น ซึ่งผู้ให้บริการจะแจ้งให้ทราบเว้นแต่กฎหมายห้าม

3.2 แจ้งผู้รับบริการโดยทันทีหากเห็นว่าคำสั่งใดอาจขัดต่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3.3 จัดให้บุคคลที่ได้รับอนุญาตให้ประมวลผลข้อมูลส่วนบุคคลผูกพันตามหน้าที่รักษาความลับ และได้รับการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

3.4 จัดให้มีและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยตามข้อ 4 และทบทวนเป็นระยะตามความเสี่ยงที่เปลี่ยนแปลงไป

3.5 จัดทำและเก็บรักษาบันทึกรายการกิจกรรมการประมวลผลตามที่กฎหมายกำหนด และพร้อมแสดงต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีคำขอโดยชอบด้วยกฎหมาย
3.6 ให้ความช่วยเหลือตามสมควรแก่ผู้รับบริการในการตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และการหารือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยผู้รับบริการรับผิดชอบค่าใช้จ่ายตามสมควรหากต้องใช้ความพยายามอย่างมีนัยสำคัญ
3.7 ไม่ขาย เปิดเผย หรือใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกจากการให้บริการตามสัญญาหลัก

ข้อ 4 มาตรการรักษาความมั่นคงปลอดภัย

4.1 ผู้ให้บริการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทางเทคนิคและเชิงองค์กรอย่างน้อยดังต่อไปนี้ ตามรายละเอียดเพิ่มเติมในคำอธิบายบริการที่เกี่ยวข้อง

ด้าน	มาตรการ
โครงสร้างพื้นฐานและการเข้ารหัส (บริการที่ผู้ให้บริการโฮสต์)	โฮสต์บนคลาวด์ของผู้ให้บริการคลาวด์ระดับองค์กรที่ได้รับการรับรอง ISO/IEC 27001 ตามรายชื่อผู้ประมวลผลช่วง ข้อมูลระหว่างส่งเข้ารหัสด้วย TLS 1.2 ขึ้นไป ข้อมูลที่จัดเก็บเข้ารหัสด้วย AES-256
การควบคุมการเข้าถึงและบุคลากร	สิทธิตามบทบาท (role-based access control) ตามหลักสิทธิน้อยที่สุด บัญชีผู้ใช้งานระบุตัวตนรายบุคคล MFA หรือ SSO ตามที่ตกลงกันใน SOW บุคลากรผูกพันรักษาความลับและเข้าถึงข้อมูลได้เฉพาะเท่าที่จำเป็นต่อการให้บริการแก่ผู้รับบริการ
การเข้าถึงสภาพแวดล้อมของผู้รับบริการ	ใช้เฉพาะวิธีการเข้าถึงและบัญชีระบุชื่อที่ผู้รับบริการจัดให้หรืออนุมัติ และให้เฉพาะบุคลากรที่จำเป็น ตามสัญญาหลัก ข้อ 12.3 ไม่เก็บสำเนาข้อมูลส่วนบุคคลไว้ในเครื่อง เว้นแต่ข้อมูลบางส่วนตามข้อ 2.2 (ข)
การตรวจสอบย้อนกลับ	สำหรับบริการที่ผู้ให้บริการโฮสต์ บันทึกการตรวจสอบ (audit trail) ที่แก้ไขไม่ได้ของการนำเข้า อ่านข้อมูล ตรวจสอบ จับคู่ แก้ไข จัดเก็บ และอนุมัติ ส่งออกเป็น CSV ได้ สำหรับซอฟต์แวร์ที่ติดตั้งในสภาพแวดล้อมของผู้รับบริการ ใช้บันทึกของซอฟต์แวร์นั้นในสภาพแวดล้อมของผู้รับบริการ
การแยกและจำกัดข้อมูล	ข้อมูลของผู้รับบริการในบริการที่ผู้ให้บริการโฮสต์แยกจากข้อมูลของลูกค้ารายอื่นในเชิงตรรกะ (logical segregation) และประมวลผลเฉพาะเอกสารและข้อมูลที่ผู้รับบริการนำเข้าสู่บริการ
การสำรองและกู้คืน	สำหรับบริการที่ผู้ให้บริการโฮสต์ สำรองข้อมูลแบบเข้ารหัสรายวัน และขั้นตอนการกู้คืนที่จัดทำเป็นเอกสารและทดสอบเป็นระยะ การสำรองข้อมูลในสภาพแวดล้อมของผู้รับบริการเป็นความรับผิดชอบของผู้รับบริการตามสัญญาหลัก ข้อ 4.2
กระบวนการพัฒนาและช่องโหว่	กระบวนการพัฒนาซอฟต์แวร์ที่ได้รับการรับรอง ISO/IEC 29110 การปรับปรุงด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ และการทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันโดยทีมภายในของผู้ให้บริการ การทดสอบเจาะระบบ (penetration test) โดยบุคคลภายนอกจัดให้เมื่อร้องขอโดยผู้รับบริการรับผิดชอบค่าใช้จ่าย
การรับมือเหตุการณ์	ขั้นตอนรับมือเหตุการณ์ที่จัดทำเป็นเอกสาร รองรับการแจ้งผู้รับบริการภายใน 48 ชั่วโมงตามข้อ 8 และการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงตามที่กฎหมายกำหนด

4.2 ผู้ให้บริการอาจปรับปรุงมาตรการข้างต้นได้ โดยไม่ลดระดับการคุ้มครองโดยรวม

ข้อ 5 ห้ามนำข้อมูลไปฝึกสอนแบบจำลองปัญญาประดิษฐ์

5.1 ผู้ให้บริการจะ **ไม่ใช้ข้อมูลของผู้รับบริการ รวมถึงข้อมูลส่วนบุคคล เพื่อฝึกสอน (train) ปรับจูน (fine-tune) หรือพัฒนาแบบจำลองปัญญาประดิษฐ์หรือแบบจำลองพื้นฐาน (foundation model) ใด** ไม่ว่าของตนเองหรือของบุคคลภายนอก และจะกำหนดค่าและทำสัญญากับผู้ให้บริการปัญญาประดิษฐ์ที่ใช้ เพื่อให้ข้อมูลที่ส่งไปประมวลผลไม่ถูกนำไปฝึกสอนแบบจำลอง ตามเงื่อนไขการใช้ข้อมูลระดับองค์กรของผู้ให้บริการเหล่านั้น การใช้ผลการตรวจสอบและแก้ไขของผู้ใช้งานและข้อมูลของผู้รับบริการเพื่อปรับปรุงกฎการตรวจสอบ กฎการจับคู่ แม่แบบ การตั้งค่า และคำสั่งประมวลผล (prompt) สำหรับการให้บริการแก่ผู้รับบริการ เป็นการตั้งค่าตามสัญญาหลัก ข้อ 9.1 ไม่ใช่การฝึกสอนหรือปรับจูนแบบจำลอง
5.2 ผู้ให้บริการอาจใช้ข้อมูลการใช้งาน (Usage Data) ในรูปแบบรวมและไม่ระบุตัวตน ซึ่งไม่มีข้อมูลส่วนบุคคล ตามที่สัญญาหลัก ข้อ 9.5 อนุญาต

ข้อ 6 ผู้ประมวลผลช่วง

6.1 ผู้รับบริการให้ความยินยอมทั่วไปแก่ผู้ให้บริการในการใช้ผู้ประมวลผลช่วง (Sub-processor) ตามรายชื่อผู้ประมวลผลช่วงของผู้ให้บริการซึ่งเผยแพร่ที่ www.sala-daeng.com/trust/sub-processors ("รายชื่อผู้ประมวลผลช่วง" (Sub-processor List)) สำหรับการโฮสต์ การจัดเก็บข้อมูล การอ่านข้อมูล (OCR) การประมวลผลด้วยปัญญาประดิษฐ์ การเข้าถึงระยะไกล และเครื่องมือสนับสนุนการใช้งาน รายชื่อผู้ประมวลผลช่วงระบุบริการ สถานที่ประมวลผล และบริการของผู้ให้บริการที่ใช้ผู้ประมวลผลช่วงแต่ละราย

6.2 ผู้ให้บริการจะ (ก) แจ้งผู้รับบริการล่วงหน้าไม่น้อยกว่า 15 วันก่อนเพิ่มหรือเปลี่ยนผู้ประมวลผลช่วง ซึ่งในระหว่างนั้นผู้รับบริการอาจคัดค้านด้วยเหตุผลอันสมควรด้านการคุ้มครองข้อมูลส่วนบุคคล โดยผู้ให้บริการแจ้งด้วยการประกาศการเปลี่ยนแปลงในรายชื่อผู้ประมวลผลช่วงพร้อมวันที่มีผล และส่งอีเมลถึงผู้ติดต่อสำหรับการบอกกล่าวของผู้รับบริการตามใบสั่งซื้อบริการ สำหรับข้อนี้ อีเมลดังกล่าวถือเป็นการแจ้งที่เพียงพอโดยไม่ต้องมีการยืนยันการรับ แม้สัญญาหลัก ข้อ 21.1 จะกำหนดไว้เป็นอย่างอื่น (ข) กำหนดให้ผู้ประมวลผลช่วงแต่ละรายมีหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลไม่น้อยกว่าข้อตกลงนี้ และ (ค) รับผิดชอบเต็มที่ต่อการปฏิบัติงานของผู้ประมวลผลช่วง หากผู้ประมวลผลช่วงรายใดหยุดหรือเปลี่ยนแปลงบริการอย่างมีนัยสำคัญ หรือจำเป็นต้องเปลี่ยนแปลงโดยเร่งด่วนเพื่อความมั่นคงปลอดภัยหรือความต่อเนื่องของบริการ ผู้ให้บริการอาจดำเนินการเปลี่ยนแปลงโดยแจ้งล่วงหน้าน้อยกว่าระยะเวลาตาม (ก) และจะแจ้งให้ผู้รับบริการทราบโดยเร็วที่สุดเท่าที่ทำได้ ทั้งนี้ ผู้รับบริการยังคงมีสิทธิตามข้อ 6.3

6.3 หากผู้รับบริการคัดค้านโดยมีเหตุอันสมควร และคู่สัญญาตกลงทางเลือกอื่นไม่ได้ภายใน 30 วัน ผู้รับบริการอาจบอกเลิกบริการส่วนที่ได้รับผลกระทบโดยแจ้งเป็นลายลักษณ์อักษร และได้รับคืนค่าบริการที่ชำระล่วงหน้าสำหรับบริการส่วนนั้นตามสัดส่วนที่ยังไม่ได้ใช้

6.4 การเปลี่ยนแบบจำลอง ผู้ให้บริการปัญญาประดิษฐ์ หรือผู้ให้บริการอ่านข้อมูล (OCR) ภายในรายชื่อผู้ประมวลผลช่วง รวมถึงการสลับระหว่างบริการของผู้ประมวลผลช่วงรายเดียวกัน ไม่ถือเป็นการเพิ่มหรือเปลี่ยนผู้ประมวลผลช่วงตามข้อ 6.2

6.5 ผู้ให้บริการโฮสต์ของผู้รับบริการเอง และผู้ให้บริการรายอื่นที่ผู้รับบริการทำสัญญาสำหรับสภาพแวดล้อมของผู้รับบริการ ไม่ใช่ผู้ประมวลผลช่วงของผู้ให้บริการ ผู้รับบริการรับผิดชอบสัญญาของตนกับผู้ให้บริการเหล่านั้น

6.6 **รายชื่อผู้ประมวลผลช่วง** รายชื่อผู้ประมวลผลช่วงแต่ละฉบับระบุวันที่มีผล ผู้ให้บริการเก็บรายชื่อฉบับก่อนหน้าไว้ให้เรียกดูได้ และจัดสำเนา PDF ของฉบับปัจจุบันให้ผู้รับบริการเมื่อร้องขอ บุคคลใดก็ตามอาจลงทะเบียนที่หน้ารายชื่อผู้ประมวลผลช่วงเพื่อรับการแจ้งตามข้อ 6.2 ทางอีเมลได้

ข้อ 7 การส่งหรือโอนข้อมูลไปต่างประเทศ

7.1 บริการที่ผู้ให้บริการโฮสต์ทำงานบนศูนย์ข้อมูลของผู้ให้บริการคลาวด์ระดับองค์กรซึ่งตั้งอยู่นอกราชอาณาจักร และผู้ให้บริการอ่านข้อมูล (OCR) และผู้ให้บริการปัญญาประดิษฐ์ประมวลผลข้อมูลนอกราชอาณาจักร ตามรายชื่อและสถานที่ประมวลผลในรายชื่อผู้ประมวลผลช่วง บริการที่ผู้ให้บริการโฮสต์จึงมีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ตามที่สัญญาหลัก ข้อ 12.2 เปิดเผยไว้และผู้รับบริการให้ความยินยอม ในลักษณะสภาพแวดล้อมของผู้รับบริการ ข้อมูลส่วนบุคคลคงอยู่ในระบบของผู้รับบริการ เว้นแต่ข้อมูลบางส่วนตามข้อ 2.2 (ข) ที่เก็บในเครื่องมือสนับสนุนของผู้ให้บริการตามรายชื่อผู้ประมวลผลช่วง

7.2 ผู้ให้บริการจะดำเนินการให้การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศเป็นไปตามมาตรา 28 และมาตรา 29 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรอง โดยการส่งไปยังประเทศปลายทางที่มีมาตรฐานการคุ้มครองที่เพียงพอตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศ การจัดให้มีมาตรการคุ้มครองที่เหมาะสม (เช่น ข้อสัญญามาตรฐานตามที่คณะกรรมการกำหนด หรือนโยบายในเครือกิจการ) หรือการอาศัยฐานอื่นที่กฎหมายอนุญาต

7.3 รายชื่อผู้ประมวลผลช่วงระบุสถานที่ประมวลผลของผู้ประมวลผลช่วงแต่ละราย การเพิ่มสถานที่ประมวลผลนอกเหนือจากที่ระบุไว้สำหรับผู้ประมวลผลช่วงรายใด ถือเป็นการเปลี่ยนแปลงตามข้อ 6.2

ข้อ 8 การละเมิดข้อมูลส่วนบุคคล

8.1 ผู้ให้บริการจะแจ้งผู้รับบริการ **โดยไม่ชักช้า และไม่ว่ากรณีใดภายใน 48 ชั่วโมง** นับแต่ทราบเหตุการละเมิดข้อมูลส่วนบุคคลที่กระทบข้อมูลของผู้รับบริการในระบบของผู้ให้บริการหรือที่เกิดจากบุคลากรของผู้ให้บริการ โดยระบุ (ในครั้งแรกหรือเป็นลำดับ) ลักษณะของการละเมิด ประเภทและปริมาณโดยประมาณของข้อมูลและเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ผลที่อาจเกิดขึ้น และมาตรการที่ได้ดำเนินการหรือเสนอให้ดำเนินการ

8.2 ผู้ให้บริการจะให้ความร่วมมือตามสมควรในการสอบสวน การแก้ไข และการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นการตัดสินใจและการดำเนินการของผู้รับบริการในฐานะผู้ควบคุมข้อมูลส่วนบุคคล สำหรับการละเมิดในสภาพแวดล้อมของผู้รับบริการที่มิได้เกิดจากผู้ให้บริการ ผู้ให้บริการจะให้ความช่วยเหลือตามสมควรเมื่อผู้รับบริการร้องขอ

ข้อ 9 การตรวจสอบ

9.1 ผู้ให้บริการจะจัดให้ผู้รับบริการได้รับข้อมูลที่จำเป็นตามสมควรเพื่อแสดงการปฏิบัติตามข้อตกลงนี้ ได้แก่ เอกสารประกอบการประเมินความมั่นคงปลอดภัยตามคำอธิบายบริการที่เกี่ยวข้อง รายชื่อผู้ประมวลผลช่วง และสำหรับบริการที่ผู้ให้บริการโฮสต์ บันทึกการตรวจสอบ (audit trail) ผ่านบทบาทผู้ตรวจสอบ (Auditor)

9.2 หากข้อมูลตามข้อ 9.1 ไม่เพียงพอ ผู้รับบริการอาจตรวจสอบการปฏิบัติตามข้อตกลงนี้ของผู้ให้บริการได้ไม่เกิน 1 ครั้งต่อรอบ 12 เดือน โดยนับรวมกับการตรวจสอบตามสัญญาหลัก ข้อ 12.6 เป็นครั้งเดียวกัน เว้นแต่หน่วยงานกำกับดูแลสั่งให้ตรวจสอบ หรือภายหลังเหตุละเมิดข้อมูลส่วนบุคคลที่ได้รับการยืนยัน โดยแจ้งล่วงหน้าไม่น้อยกว่า 20 วันทำการ ดำเนินการในเวลาทำการ และผู้รับบริการรับผิดชอบค่าใช้จ่าย การตรวจสอบอยู่

ภายใต้นโยบายความมั่นคงปลอดภัยและการรักษาความลับของผู้ให้บริการ และไม่ครอบคลุมข้อมูลของลูกค้ารายอื่น ข้อมูลต้นทุนของผู้ให้บริการ หรือรหัสต้นฉบับ (source code) ของซอฟต์แวร์ของผู้ให้บริการ

ข้อ 10 การส่งคืนและการลบข้อมูล

10.1 เมื่อสิ้นสุดหรือเลิกสัญญาหลักหรือใบสั่งซื้อบริการที่เกี่ยวข้อง ผู้ให้บริการจะส่งคืนข้อมูลของผู้รับบริการ และ/หรือ ลบข้อมูลและสำเนาที่เหลืออยู่ ตามที่ผู้รับบริการเลือก ภายในกำหนดเวลาและวิธีการตามสัญญาหลัก ข้อ 17 เว้นแต่กฎหมายไทยกำหนดให้เก็บรักษา ซึ่งข้อ 3 ยังคงใช้บังคับกับข้อมูลที่เก็บรักษานั้น สำเนาสำรองถูกลบตามรอบการหมุนเวียนตามปกติและได้รับการคุ้มครองจนกว่าจะถูกลบ
10.2 หากผู้รับบริการสั่งให้เก็บรักษาข้อมูลตามนโยบายการเก็บรักษาเอกสารของตน (เช่น เอกสารภาษีไม่น้อยกว่า 5 ปีตามข้อกำหนดของกรมสรรพากร) ระหว่างที่บริการยังมีผลอยู่ ผู้ให้บริการจะเก็บรักษาตามคำสั่ง และข้อตกลงนี้ใช้บังคับตลอดระยะเวลาดังกล่าว
10.3 **ข้อมูลบางส่วนที่นำออก** ผู้ให้บริการลบข้อมูลบางส่วนที่นำออกเพื่อการโอนย้ายข้อมูลและการทดสอบภายใน 30 วันนับแต่วันเริ่มใช้งานจริง (Go-Live) ของระยะงานที่ข้อมูลนั้นใช้ ข้อมูลส่วนบุคคลในรายการแจ้งปัญหาเก็บไว้พร้อมประวัติรายการแจ้งปัญหาระหว่างที่บริการยังมีผลอยู่ และลบตามข้อ 10.1 เมื่อบริการสิ้นสุด เมื่อผู้รับบริการร้องขอ ผู้ให้บริการจะยืนยันการลบเป็นลายลักษณ์อักษร

ข้อ 11 ความรับผิด

ความรับผิดภายใต้ข้อตกลงนี้อยู่ภายใต้ข้อจำกัดความรับผิดตามสัญญาหลัก ข้อ 15

ข้อ 12 ระยะเวลาและเวอร์ชัน

12.1 ข้อตกลงนี้มีผลตั้งแต่วันที่สัญญาหลักมีผล และมีผลต่อไปตราบเท่าที่ผู้ให้บริการยังประมวลผลข้อมูลส่วนบุคคลในนามของผู้รับบริการ รวมถึงระยะเวลาส่งคืนและลบข้อมูลตามข้อ 10
12.2 ผู้ให้บริการอาจประกาศข้อตกลงเวอร์ชันใหม่สำหรับใบสั่งซื้อบริการฉบับใหม่ได้ การเปลี่ยนแปลงข้อตกลงนี้สำหรับใบสั่งซื้อบริการที่มีผลอยู่ต้องทำเป็นลายลักษณ์อักษรและลงนามโดยคู่สัญญาทั้งสองฝ่าย เว้นแต่การปรับปรุงรายชื่อผู้ประมวลผลช่วงตามข้อ 6.2 และการปรับปรุงที่จำเป็นตามกฎหมาย ซึ่งผู้ให้บริการจะแจ้งให้ทราบ
12.3 **การตกลงและการลงนาม** คู่สัญญาตกลงตามข้อตกลงนี้โดยการลงนามในใบสั่งซื้อบริการที่อ้างถึงข้อตกลงนี้ โดยไม่ต้องลงนามในข้อตกลงนี้แยกต่างหาก เมื่อผู้รับบริการร้องขอ ผู้ให้บริการจะจัดสำเนาที่ผู้ให้บริการลงนามแล้วให้
12.4 **ภาษา** ผู้ให้บริการเผยแพร่ข้อตกลงนี้เป็นภาษาไทยและภาษาอังกฤษ ซึ่งมีเนื้อหาเดียวกันภายใต้เลขเวอร์ชันเดียวกัน และให้ใช้ภาษาของสัญญาหลักที่ผู้รับบริการลงนามเป็นหลัก

เอกสารแนบ DPA-1 รายละเอียดการประมวลผล

เอกสารแนบนี้กำหนดรายละเอียดมาตรฐานสำหรับลักษณะการประมวลผลแต่ละแบบตามข้อ 2.2 ส่วนการประมวลผลข้อมูลส่วนบุคคลในใบสั่งซื้อบริการระบุว่าลักษณะใดใช้บังคับ และรายการเพิ่มเติม ซึ่งให้ถือเป็นส่วนหนึ่งของเอกสารแนบนี้สำหรับผู้รับบริการรายนั้น

หัวข้อ	บริการที่ผู้ให้บริการโฮสต์	สภาพแวดล้อมของผู้รับบริการ
เรื่องที่ประมวลผล	การให้บริการที่ผู้ให้บริการโฮสต์ตามใบสั่งซื้อบริการ เช่น BackOffice IQ	การติดตั้ง บำรุงรักษา และสนับสนุน SAP Business One และซอฟต์แวร์ของผู้ให้บริการที่ทำงานในสภาพแวดล้อมของผู้รับบริการ
ระยะเวลา	ตลอดอายุสัญญาหลักและใบสั่งซื้อบริการที่เกี่ยวข้อง รวมระยะเวลาส่งคืนและลบข้อมูลตามข้อ 10	เช่นเดียวกัน
ลักษณะและวัตถุประสงค์	การนำเข้าและแยกเอกสาร การอ่านข้อมูล (OCR) การจำแนกประเภท การสกัดข้อมูลรายฟิลด์ การตรวจสอบความถูกต้อง การตรวจสอบข้อมูลคู่ค้า (รวมถึงการสอบถามฐานข้อมูลสาธารณะของหน่วยงานรัฐ) การจับคู่กับข้อมูลอ้างอิงจากระบบบัญชีของผู้รับบริการ การจัดเก็บเอกสาร บันทึกการตรวจสอบ การส่งออกข้อมูล และการสนับสนุน	การตั้งค่าระบบ การโอนย้ายข้อมูลหลักและยอดยกมา การทดสอบ การฝึกอบรม การเชื่อมต่อข้อมูลตามรอบเวลา การสนับสนุนและแก้ไขปัญหา การบำรุงรักษาและการปรับปรุงรุ่น
เจ้าของข้อมูลส่วนบุคคล	บุคลากรและผู้แทนของคู่ค้าของผู้รับบริการ คู่ค้าที่เป็นบุคคลธรรมดา และพนักงานของผู้รับบริการที่ใช้งานบริการ	พนักงานและผู้ใช้งานระบบของผู้รับบริการ ผู้ติดต่อของผู้ขายและลูกค้า ผู้ขายและลูกค้าที่เป็นบุคคลธรรมดา

หัวข้อ	บริการที่ผู้ให้บริการโฮสต์	สภาพแวดล้อมของผู้รับบริการ
ประเภทข้อมูลส่วนบุคคล	ชื่อ ตำแหน่ง ลายมือชื่อ และข้อมูลติดต่อ (ที่อยู่ โทรศัพท์ อีเมล) เลขประจำตัวผู้เสียภาษีของบุคคลธรรมดา ข้อมูลบัญชีธนาคารที่ปรากฏบนเอกสาร ข้อมูลบัญชีผู้ใช้งาน (ชื่อ อีเมล บทบาท ประวัติการใช้งาน)	ชื่อ ตำแหน่ง ลายมือชื่อ และข้อมูลติดต่อ เลขประจำตัวผู้เสียภาษีของบุคคลธรรมดา ข้อมูลบัญชีธนาคารสำหรับการจ่ายเงินและการคืนเงิน ใบแจ้งหนี้ ใบเสร็จรับเงิน และประวัติการชำระเงิน ข้อมูลบัญชีผู้ใช้งาน (ชื่อ อีเมล บทบาท ประวัติการใช้งาน)
ข้อมูลส่วนบุคคลอ่อนไหว	ไม่มีโดยเจตนา หากปรากฏในเอกสารโดยบังเอิญจะถูกประมวลผลเฉพาะในฐานะส่วนหนึ่งของภาพเอกสาร และไม่ถูกสกัดออกมาเป็นข้อมูล	ไม่มี เว้นแต่ใบสั่งซื้อบริการระบุไว้ ฟิลด์ที่เก็บข้อมูลอ่อนไหวในระบบต้นทางจะไม่ถูกเชื่อมต่อเข้ามา
การยืนยันตัวตน	MFA หรือ SSO ตามที่ตกลงกันใน SOW หรือใบสั่งซื้อบริการ	ตามที่ระบบของผู้รับบริการรองรับ โดยใช้วิธีการเข้าถึงตามสัญญาหลัก ข้อ 12.3

เอกสารแนบ DPA-2 ผู้ประมวลผลช่วง

ผู้ประมวลผลช่วงที่ได้รับอนุมัติ ได้แก่ ผู้ประมวลผลช่วงตามรายชื่อผู้ประมวลผลช่วง (ข้อ 6.1) ที่ www.sala-daeng.com/trust/sub-processors ผู้ให้บริการโฮสต์ของผู้รับบริการเองและผู้ให้บริการรายอื่นที่ผู้รับบริการทำสัญญาสำหรับสภาพแวดล้อมของผู้รับบริการ ไม่ใช่ผู้ประมวลผลช่วงของผู้ให้บริการ (ข้อ 6.5)