การวิเคราะห์ · 26 พฤษภาคม 2026

← ก่อนหน้า·ถัดไป →

ความเป็นส่วนตัวจริง vs ที่ดูเหมือนจริง: คำถามที่ควรถามตัวเอง

บทสรุปเชิงปฏิบัติของวงรอบที่ 2: คำถามที่แยกแยะบริการที่มีความเป็นส่วนตัวเชิงสถาปัตยกรรมออกจากบริการที่มีความเป็นส่วนตัวเชิงคำประกาศ แบบสอบถามสำหรับมืออาชีพชาวยุโรปก่อนที่จะนำเครื่องมือดิจิทัลใด ๆ มาใช้กับข้อมูลอ่อนไหว

เพื่อให้เข้าใจตรงกัน: สองบริการที่มีประกาศทางกฎหมายเดียวกันอาจประพฤติแตกต่างกันอย่างมาก แบบหนึ่งปกป้องด้วยการออกแบบทางเทคนิค อีกแบบหนึ่งปกป้องด้วยคำสัญญาตามสัญญา ความแตกต่างนั้นไม่ได้อ่านได้จากประกาศ — แต่ค้นพบได้ด้วยการตั้งคำถามที่เป็นรูปธรรม คุณภาพของคำตอบบอกถึงตัวผลิตภัณฑ์ได้พอ ๆ กับเนื้อหาของมันเอง

ความแตกต่างระหว่างความเป็นส่วนตัวเชิงสถาปัตยกรรมกับความเป็นส่วนตัวเชิงคำประกาศ

ตลอดเจ็ดบทความก่อนหน้าในวงรอบนี้ เราได้ผ่านชั้นต่าง ๆ ของเรื่องเดียวกัน กฎหมายว่าด้วยการถ่ายโอนข้อมูลระหว่างประเทศกับ Schrems II แนวคิดทางคณิตศาสตร์ของแฮชการเข้ารหัสที่ผนึก Cuaderno แต่ละเล่ม ทางเลือกเชิงสถาปัตยกรรมของ kill switch และการยึดกุมโดยสถาบันที่มักมาคู่กันเสมอ กลไกของการเข้ารหัสแบบ end-to-end และคำถามเชิงปฏิบัติว่ากุญแจอยู่ที่ใด การจัดวางแรงจูงใจให้สอดคล้องตามโมเดลธุรกิจ อัตลักษณ์การเข้ารหัสแบบอธิปไตยในตนเอง การโฮสต์ด้วยตนเองในฐานะกลยุทธ์ที่ได้สัดส่วน แต่ละบทความจัดการกับมุมหนึ่ง บทความนี้ ซึ่งเป็นบทสุดท้ายของวงรอบ รวบรวมทั้งหมดไว้ในแบบสอบถามเดียว

ความแตกต่างที่ควรจดจำนั้นเรียบง่าย: มีบริการที่ความเป็นส่วนตัวเป็นแบบ *เชิงสถาปัตยกรรม* และมีบริการที่ความเป็นส่วนตัวเป็นแบบ *เชิงคำประกาศ* แบบแรกฝังอยู่ในการออกแบบทางเทคนิค: การละเมิดข้อผูกพันด้านความเป็นส่วนตัวบางอย่างเป็นเรื่องยากหรือเป็นไปไม่ได้ในทางเทคนิค เพราะสถาปัตยกรรมไม่อนุญาตให้ทำ แบบที่สองฝากไว้ในข้อความของประกาศทางกฎหมาย: การละเมิดบางอย่างจะลงโทษได้ตามสัญญาหากเกิดขึ้น แต่ในทางเทคนิคไม่มีสิ่งใดขัดขวางมัน ทั้งสองโมเดลสามารถปฏิบัติตาม GDPR ได้

แต่แบบหนึ่งปกป้องด้วยการสร้างขึ้น และอีกแบบหนึ่งปกป้องด้วยคำสัญญา และความแตกต่างนั้นมหาศาลในเชิงปฏิบัติ

คำถามที่ตามมาออกแบบมาเพื่อแยกแยะกรณีหนึ่งจากอีกกรณีหนึ่ง มันไม่ใช่คำถามทางเทคนิคขั้นสูง มันคือคำถามที่ผู้ให้บริการที่ซื่อสัตย์คนใดก็ตามสามารถตอบได้ในเอกสารสาธารณะของตน คุณภาพและความแม่นยำของคำตอบบอกถึงตัวผลิตภัณฑ์ได้พอ ๆ กับคำตอบนั้นเอง คำถามถูกจัดกลุ่มเป็นหกชั้น ควรถามให้ครบทุกข้อก่อนนำบริการมาใช้กับข้อมูลอ่อนไหว ไม่ใช่เฉพาะข้อที่สัญชาตญาณแรกระบุได้

ชั้นที่ 1: สถาปัตยกรรม

ก่อนจะไปต่อ ขอกำหนดคำหนึ่งให้ชัดก่อน *ผู้ให้บริการ* ในที่นี้หมายถึงบริษัทที่ให้บริการ องค์กรที่ควบคุมเซิร์ฟเวอร์และซอฟต์แวร์ ไม่ใช่บุคคลใดบุคคลหนึ่ง เมื่อชัดเจนเช่นนี้แล้ว คำถามเชิงสถาปัตยกรรมพื้นฐานคือ: ผู้ให้บริการทำอะไรกับเนื้อหาที่อยู่ระหว่างผู้ส่งและผู้รับ? มีคำตอบที่เป็นไปได้สามแบบ และควรรู้จักแยกแยะให้ออก เพราะทั้งสามแบบบางครั้งถูกโฆษณาด้วยถ้อยคำที่คล้ายกัน

- แบบแรก: เนื้อหาผ่านเซิร์ฟเวอร์ของผู้ให้บริการแบบไม่เข้ารหัส ซึ่งผู้ให้บริการสามารถอ่านมันได้แม้จะสัญญาว่าจะไม่ทำ
- แบบที่สอง: เนื้อหาผ่านเซิร์ฟเวอร์ของผู้ให้บริการแบบเข้ารหัส ซึ่งผู้ให้บริการไม่สามารถอ่านมันได้ หากกุญแจอยู่ในอุปกรณ์ของผู้ใช้แต่เพียงผู้เดียว
- แบบที่สาม: เนื้อหาไม่ผ่านเซิร์ฟเวอร์ของผู้ให้บริการใด ๆ เพราะไม่มีเซิร์ฟเวอร์ของผู้ให้บริการในกระแสการไหลนั้นโดยเฉพาะ

ความแตกต่างระหว่างทั้งสามแบบนี้ไม่ใช่เรื่องของระดับ แต่เป็นเรื่องของชนิด

คำถามเสริม —ซึ่งได้ตั้งไว้แล้วใน Cuaderno ว่าด้วยการเข้ารหัส— คือ: ใครมีกุญแจการเข้ารหัสที่ทำให้อ่านเนื้อหาได้? หากผู้ใช้มีมันและมีแต่ผู้ใช้เท่านั้น การเข้ารหัสก็เป็นของจริง หากผู้ให้บริการมีมันด้วยในรูปแบบใด ๆ —แม้จะอยู่ภายใต้ชื่อ «การกู้คืนบัญชี» หรือ «การซิงค์ระหว่างอุปกรณ์»— การเข้ารหัสก็เป็นเพียงในนาม คำถามนี้ไม่ยอมรับคำตอบกลาง ๆ ที่ซื่อสัตย์

ชั้นที่ 2: โมเดลธุรกิจ

คำถามเกี่ยวกับโมเดลธุรกิจมีความสำคัญพอ ๆ กับคำถามเชิงสถาปัตยกรรม และด้วยเหตุผลสาระสำคัญเดียวกัน: แรงจูงใจก่อให้เกิดผลิตภัณฑ์ที่แตกต่างกันอย่างเป็นระบบตลอดช่วงเวลา แม้จะมีวัตถุประสงค์ที่ประกาศไว้เหมือนกันก็ตาม วันนี้ผู้ให้บริการหารายได้อย่างไร? แหล่งเดียว สองแหล่ง หรือผสมกัน? หากการหารายได้รวมถึงโฆษณาหรือการสร้างมูลค่าจากข้อมูล มีการสร้างมูลค่าจากข้อมูลใด และทำบนฐานทางกฎหมายใดของ GDPR? วัตถุประสงค์ที่ประกาศไว้ในประกาศทางกฎหมายครอบคลุมข้อมูลของบุคคลที่สามที่มืออาชีพตั้งใจจะมอบความไว้วางใจให้บริการหรือไม่?

และคำถามลำดับที่สอง ซึ่งไม่ได้ตั้งไว้เสมอไป: สถานะทางการเงินของผู้ให้บริการในระยะสามถึงห้าปีข้างหน้าเป็นอย่างไร? บริษัทในระยะเงินร่วมลงทุนดำเนินงานภายใต้แรงกดดันที่ต่างจากบริษัทที่มีผลกำไรมั่นคง การเปลี่ยนแปลงโมเดลการระดมทุนเป็น ซ้ำแล้วซ้ำเล่า ช่วงเวลาที่สัญญาโดยปริยายกับผู้ใช้ถูกเขียนขึ้นใหม่โดยไม่มีการเจรจา

ชั้นที่ 3: เขตอำนาจศาล

สำหรับมืออาชีพชาวยุโรป คำถามเรื่องเขตอำนาจศาลไม่ใช่เรื่องวาทศิลป์ ผู้ให้บริการจดทะเบียนในเขตอำนาจศาลใด? เซิร์ฟเวอร์ที่ประมวลผลข้อมูลตั้งอยู่จริงในประเทศใด? คำตอบของสองคำถามก่อนหน้าเหมือนหรือต่างกัน และหากต่างกัน กฎหมายใดที่ใช้บังคับ? ภูมิภาคของยุโรปที่ดำเนินการโดยบริษัทอเมริกันไม่ถือเป็นคำตอบแบบยุโรปในแง่ของ Schrems II: บริษัทอยู่ภายใต้ FISA 702 ไม่ว่าเซิร์ฟเวอร์จะตั้งอยู่ที่ใดก็ตาม

คำถามเสริมเชิงปฏิบัติคือ: หากพรุ่งนี้มีคำสั่งด้านข่าวกรองที่ชอบด้วยกฎหมายในเขตอำนาจศาลของผู้ให้บริการมาถึง โดยเรียกร้องให้ส่งมอบข้อมูลของฉันหรือของลูกค้าฉัน จะเกิดอะไรขึ้น? หากคำตอบที่ซื่อสัตย์เริ่มต้นด้วย «บริษัทจะมีหน้าที่ต้องส่งมอบมัน» บริการนั้นก็ไม่ได้ปกป้องจากคำสั่งนั้น ไม่ว่าโฆษณาจะบอกเป็นนัยตรงกันข้ามมากเพียงใด หากคำตอบที่ซื่อสัตย์เริ่มต้นด้วย «บริษัทไม่สามารถส่งมอบมันได้เพราะไม่มีมันในรูปแบบไม่เข้ารหัส» บริการนั้นก็ปกป้องจริง และความแตกต่างนั้นขึ้นอยู่กับสองชั้นแรกเกือบทั้งหมด ไม่ใช่คุณภาพของนโยบายความเป็นส่วนตัว

ชั้นที่ 4: ผู้ให้บริการและ kill switch

ผู้ให้บริการคงไว้ซึ่งขีดความสามารถทางเทคนิคใดในการระงับ ปิดกั้น ลบ หรือลดทอนบริการจากระยะไกล? คำถามนี้ไม่ใช่ความหวาดระแวง แต่เป็นเรื่องเชิงปฏิบัติ แพลตฟอร์มดิจิทัลได้ใช้ขีดความสามารถนั้นซ้ำแล้วซ้ำเล่าในช่วงไม่กี่ปีที่ผ่านมา บางครั้งด้วยความริเริ่มของตนเอง บางครั้งภายใต้คำสั่งของรัฐบาล บางครั้งหลังจากการเปลี่ยนแปลงเจ้าของหรือนโยบาย หากขีดความสามารถนั้นมีอยู่ ควรรู้ว่ามันถูกใช้ภายใต้เงื่อนไขที่ประกาศไว้ตามสัญญาใด และสำรองพื้นที่ไว้สำหรับเงื่อนไขที่ไม่ได้ประกาศซึ่งการปฏิบัติในช่วงไม่กี่ปีที่ผ่านมาได้แสดงให้เห็นว่ามีความสำคัญไม่แพ้กัน: คำสั่งศาลที่ไม่คาดคิด การคว่ำบาตรระหว่างประเทศ การเปลี่ยนแปลงการกำกับดูแลกิจการ การถูกซื้อกิจการโดยองค์กรที่มีนโยบายอื่น

คำถามคู่กันคือเรื่องแผนความต่อเนื่อง: หากผู้ให้บริการใช้ขีดความสามารถนั้นต่อมืออาชีพ —ด้วยเหตุผลใดก็ตาม ชอบธรรมหรือไม่ก็ตาม— จะยังคงมีเวลาใช้งานเหลืออยู่เท่าใด มีขั้นตอนการส่งออกข้อมูลอะไรอยู่ และจะย้ายไปยังผู้ให้บริการรายอื่นใดได้บ้าง? หากคำตอบเริ่มต้นด้วย «มันไม่ควรเกิดขึ้น» นั่นไม่ใช่คำตอบเชิงปฏิบัติ แต่เป็นคำสัญญา

ชั้นที่ 5: อัตลักษณ์และการเข้าถึง

ใครควบคุมข้อมูลรับรองการเข้าถึงบริการ? หากผู้ให้บริการสามารถรีเซ็ตการเข้าถึงของผู้ใช้ได้โดยไม่ต้องมีส่วนร่วมจากผู้ใช้ —ขั้นตอนที่มักเรียกว่า «การกู้คืนบัญชี»— ผู้ให้บริการคือผู้ดูแลบัญชีในทางเทคนิค และยังสามารถมอบบัญชีนั้นให้แก่ผู้ที่ร้องขอผ่านขั้นตอนที่เหมาะสมได้ด้วย หากผู้ให้บริการไม่สามารถรีเซ็ตการเข้าถึงได้เพราะอัตลักษณ์อยู่เชิงการเข้ารหัสในอุปกรณ์ของผู้ใช้ ผู้ให้บริการก็ไม่สามารถมอบมันให้ได้เช่นกัน แม้แต่ภายใต้คำสั่ง ทั้งสองรูปแบบชอบธรรมตามบริบท แต่ก็แตกต่างกันอีกครั้ง และควรรู้ว่ากำลังนำรูปแบบใดมาใช้

จะเกิดอะไรขึ้นกับข้อมูลของมืออาชีพหากมืออาชีพสูญเสียการเข้าถึง? มีกลไกการกู้คืน —บัญชี ไฟล์ เซสชัน— ที่ขึ้นอยู่กับผู้ให้บริการหรือไม่? กลไกเหล่านั้นสอดคล้องกับจรรยาบรรณวิชาชีพของภาคส่วนนั้นหรือไม่ หากผู้ให้บริการถูกบีบบังคับให้ใช้มัน?

ชั้นที่ 6: อนาคต

ชั้นสุดท้ายนี้มักถูกละเลยเพราะมันต้องอาศัยการคาดการณ์ จะเกิดอะไรขึ้นหากบริการถูกซื้อกิจการโดยบริษัทอื่น? เกือบทุกการเข้าซื้อกิจการมาพร้อมกับการทบทวนเงื่อนไขการให้บริการในเดือนต่อ ๆ มา จะเกิดอะไรขึ้นหากข้อกำหนดด้านการกำกับดูแลเปลี่ยนไป? กฎหมายยุโรปได้เพิ่มภาระหน้าที่ในการถอดถอนและปิดกั้นตั้งแต่ปี 2022 ไม่ได้ลดลง จะเกิดอะไรขึ้นหากผู้ให้บริการหายไป? บริการคลาวด์ส่วนใหญ่จำนวนไม่น้อยไม่มีแผนทางออกที่บันทึกไว้สำหรับสถานการณ์ที่ผู้ให้บริการปิดตัวลง มืออาชีพค้นพบปัญหานี้เมื่อไม่มีเวลาเตรียมการอีกแล้ว

มีการกล่าวรูปแบบหนึ่งที่ควรจดจำไว้สำหรับชั้นนี้: สถาปัตยกรรมที่พึ่งพาผู้ให้บริการน้อยลงย่อมยืดหยุ่นต่อการเปลี่ยนแปลงของผู้ให้บริการมากขึ้น การโฮสต์ด้วยตนเองในรูปแบบใดก็ตาม อัตลักษณ์การเข้ารหัสแบบอธิปไตยในตนเอง การสื่อสารที่ไม่มีเซิร์ฟเวอร์อยู่ตรงกลาง ทั้งหมดนี้ลดพื้นที่ความเสี่ยงในอนาคตด้วยกระบวนการลดพื้นที่การพึ่งพาในปัจจุบัน มันไม่ได้ขจัดความเสี่ยง แต่มันลดความเสี่ยง

ความแตกต่างระหว่างโครงสร้างกับคำสัญญา

หากเราต้องกลั่นวงรอบนี้ให้เหลือเพียงประโยคเดียว มันจะเป็นประโยคนี้: คำตอบเชิงโครงสร้างยังคงอยู่แม้ผู้ให้บริการ ฝ่ายบริหาร หรือกฎหมายจะเปลี่ยนไป คำตอบโดยคำสัญญายังคงอยู่ตราบเท่าที่ผู้ให้สัญญายังสามารถและยังต้องการรักษามันไว้ ทั้งสองอาจถูกต้องในขณะที่นำมาใช้ แต่มีเพียงหนึ่งในสองเท่านั้นที่ดำรงอยู่ได้โดยไม่ขึ้นกับกาลเวลาที่ผ่านไปและการเปลี่ยนแปลงของสถานการณ์

นี่ไม่ได้หมายความว่ามืออาชีพแต่ละคนจะต้องเรียกร้องคำตอบเชิงโครงสร้างจากทุกบริการที่นำมาใช้ ความได้สัดส่วนยังคงชอบธรรม: สเปรดชีตสำหรับบัญชีภายในไม่จำเป็นต้องมีคำตอบแบบเดียวกับเวชระเบียนของผู้ป่วย แต่มันหมายความว่า ความเป็นมืออาชีพอยู่ที่การรู้ว่าได้ยอมรับคำตอบชนิดใดในแต่ละกรณี และได้ตัดสินใจอย่างมีสติว่าคำตอบชนิดนั้นได้สัดส่วนกับข้อมูลที่เป็นรูปธรรมนั้น

แบบสอบถาม เรียงตามลำดับ

สิบสองคำถามที่เป็นรูปธรรมซึ่งสรุปวงรอบนี้ เรียงลำดับเพื่อให้คำตอบของแต่ละข้อให้ข้อมูลแก่ข้อถัดไป:

1. เนื้อหาผ่านเซิร์ฟเวอร์ของผู้ให้บริการหรือไม่? ถ้าผ่าน: เป็นแบบไม่เข้ารหัส เข้ารหัสด้วยกุญแจของผู้ให้บริการ หรือเข้ารหัสด้วยกุญแจเฉพาะของผู้ใช้?
2. หากมีการอ้างถึงการเข้ารหัสแบบ end-to-end กุญแจการเข้ารหัสอยู่ที่ใด? ผู้ให้บริการรู้หรือเก็บส่วนใดส่วนหนึ่งของมันไว้ในรูปแบบใด ๆ รวมถึงในรูปของ «การกู้คืน» หรือไม่?
3. บริการสร้างและเก็บ Metadata อะไรบ้าง? นานเท่าใด? ใครมองเห็นได้บ้าง?
4. ผู้ให้บริการหารายได้อย่างไร? หากการหารายได้รวมถึงโฆษณาหรือการสร้างมูลค่าจากข้อมูล วัตถุประสงค์ที่ประกาศไว้ครอบคลุมข้อมูลของบุคคลที่สามที่มืออาชีพมอบความไว้วางใจไว้หรือไม่?
5. สถานะทางการเงินของผู้ให้บริการในระยะสามถึงห้าปีข้างหน้าเป็นอย่างไร? มีปัจจัยใดที่บ่งชี้ถึงการเปลี่ยนโมเดลที่ใกล้จะเกิดขึ้นหรือไม่ (การเข้าตลาดหลักทรัพย์ที่ค้างอยู่ รอบระดมทุนที่กำลังหมดลง การถูกซื้อกิจการที่น่าจะเกิดขึ้น)?
6. ผู้ให้บริการจดทะเบียนในเขตอำนาจศาลใด? เซิร์ฟเวอร์ตั้งอยู่จริงในประเทศใด? หากต่างกัน กฎหมายของประเทศใดที่ใช้บังคับกับการประมวลผล?
7. จะเกิดอะไรขึ้นหากคำสั่งด้านข่าวกรองที่ชอบด้วยกฎหมายในเขตอำนาจศาลของผู้ให้บริการเรียกร้องให้ส่งมอบข้อมูลของฉัน? บริษัทสามารถปฏิบัติตามได้ในทางเทคนิคหรือไม่?
8. ผู้ให้บริการคงไว้ซึ่งขีดความสามารถทางเทคนิคใดในการระงับ ปิดกั้น หรือลบบริการ? ภายใต้เงื่อนไขตามสัญญาใด? ภายใต้เงื่อนไขนอกสัญญาใดที่มีการบันทึกไว้ในอดีต?
9. มีแผนทางออกอะไรหากผู้ให้บริการใช้ขีดความสามารถนั้นต่อฉัน ไม่ว่าจะโดยชอบหรือไม่ชอบธรรม? มีขั้นตอนการส่งออกข้อมูลไปยังผู้ให้บริการรายอื่นที่บันทึกไว้หรือไม่?
10. ใครควบคุมข้อมูลรับรองการเข้าถึง? ผู้ให้บริการสามารถรีเซ็ตมันได้โดยไม่ต้องมีส่วนร่วมจากฉันหรือไม่? สิ่งนั้นปกป้องฉันหรือเปิดเผยฉัน?
11. มีทางเลือกแบบยุโรป แบบโฮสต์ด้วยตนเอง หรือแบบไม่มีเซิร์ฟเวอร์อยู่ตรงกลางสำหรับฟังก์ชันนี้โดยเฉพาะหรือไม่? ต้นทุนที่แท้จริงของมันคือเท่าไร เมื่อเทียบกับความเสี่ยงที่ประเมินไว้?
12. หากการตัดสินใจในวันนี้ถูกตรวจสอบในอีกห้าปีข้างหน้าโดยผู้ตรวจการ ผู้สอบบัญชี หรือลูกค้าที่ได้รับผลกระทบจากการรั่วไหล การเลือกในปัจจุบันจะปกป้องได้ด้วยข้อโต้แย้งที่มีอยู่ในวันนี้ หรือจะต้องขอโทษที่ไม่ได้ตั้งคำถามที่สมเหตุสมผล?

คำถามเหล่านี้ไม่ได้คาดหวังคำตอบที่สมบูรณ์แบบ มันคาดหวังคำตอบที่ซื่อสัตย์ ซึ่งผู้ให้บริการที่ซื่อสัตย์รู้ว่าจะตอบอย่างไร และผู้ให้บริการที่ซื่อสัตย์น้อยกว่าจะหลีกเลี่ยงการระบุอย่างแม่นยำ ความแตกต่างเชิงปฏิบัติระหว่างผู้ให้บริการทั้งสองชนิด เราพูดโดยปราศจากการสร้างดราม่า มักรับรู้ได้จากการอ่านคำตอบที่พวกเขาเสนอให้โดยสมัครใจอย่างช้า ๆ ก่อนที่จะต้องขอข้อมูลเพิ่มเติมเสียด้วยซ้ำ

ด้วยบทความนี้ เราปิดวงรอบที่สองของ Cuadernos Lacre เราเริ่มต้นด้วยหนี้ทางบรรณาธิการที่สืบทอดมาจาก Schrems II และจบลงด้วยแบบสอบถามเชิงปฏิบัติ ระหว่างทางเราได้ผ่านแนวคิดต่าง ๆ —แฮช การเข้ารหัส อัตลักษณ์— และการวิเคราะห์ที่นำไปใช้จริง —kill switch โมเดลธุรกิจ การโฮสต์ด้วยตนเอง— เจตนาทางบรรณาธิการที่ประกาศไว้ของสิ่งพิมพ์นี้ไม่ได้อยู่ที่การถาโถมผู้อ่านด้วยรายการปัญหาที่ครบถ้วนสมบูรณ์ แต่อยู่ที่การมอบเครื่องมือให้เขาแยกแยะได้ว่า เมื่อเผชิญกับบริการใหม่ใด ๆ เขากำลังยอมรับคำตอบชนิดใด การแยกแยะนั้น —ระหว่างสถาปัตยกรรมกับคำสัญญา— คือเครื่องมือ ส่วนที่เหลือ มืออาชีพแต่ละคนจะนำไปใช้กับข้อมูลที่เขาเห็นว่า ในการปฏิบัติงานของเขา สมควรแก่คำถามนั้น

แหล่งข้อมูลและการอ่านเพิ่มเติม

- สิ่งพิมพ์นี้ วงรอบที่ 2 (พฤษภาคม 2026) — *Schrems II ห้าปีให้หลัง*, *SHA-256 คืออะไรกันแน่*, *Kill switch และการยึดกุมโดยสถาบัน*, *การเข้ารหัสแบบ end-to-end อธิบายอย่างแท้จริง*, *โมเดลธุรกิจในฐานะสัญญาณแห่งความไว้วางใจ*, *24 คำ: อัตลักษณ์การเข้ารหัสคืออะไร*, *Self-hosting ในฐานะแนวปฏิบัติทางวิชาชีพ* เจ็ดบทความที่แบบสอบถามนี้ตั้งอยู่บน
- ข้อบังคับ (สหภาพยุโรป) 2016/679 — ข้อบังคับว่าด้วยการคุ้มครองข้อมูลทั่วไป กรอบทางกฎหมายอ้างอิงสำหรับทุกคำถามที่แบบสอบถามตั้งขึ้น โดยเฉพาะมาตรา 5, 6, 25, 28, 32, 33 และบทที่ 5
- คณะกรรมการคุ้มครองข้อมูลแห่งยุโรป — แนวปฏิบัติและความเห็นเชิงปฏิบัติเกี่ยวกับ Schrems II การถ่ายโอนข้อมูลระหว่างประเทศ การประเมินผลกระทบ และความรับผิดชอบเชิงรุก (สิ่งพิมพ์ปี 2020-2024)
- หน่วยงานคุ้มครองข้อมูลแห่งสเปน — บทลงโทษที่เผยแพร่ปี 2022-2024 ต่อผู้ควบคุมข้อมูลจากการใช้เครื่องมือถ่ายโอนข้อมูลที่ไม่เหมาะสม หรือจากการประเมินผลกระทบที่เป็นทางการแต่ไร้เนื้อหาสาระ
- noyb.eu — ศูนย์ยุโรปเพื่อสิทธิดิจิทัล นำโดย Maximilian Schrems คลังสาธารณะของข้อร้องเรียน คำอุทธรณ์ และบทวิเคราะห์เกี่ยวกับการปฏิบัติตามกฎการคุ้มครองข้อมูลของยุโรปอย่างแท้จริง ไม่ใช่เพียงในรูปลักษณ์ภายนอก

← ก่อนหน้าSelf-hosting ในฐานะการปฏิบัติทางวิชาชีพถัดไป →สิ่งที่ลายเซ็นไม่สามารถแก้ไขได้

บทความล่าสุด

- บทสะท้อนความคิด · 29 มิถุนายน 2026 คุณไม่ได้เป็นนิรนาม
- บทสะท้อน · 27 พฤษภาคม 2026 สิ่งที่ลายเซ็นไม่สามารถแก้ไขได้
- การวิเคราะห์ · 25 พฤษภาคม 2026 Self-hosting ในฐานะการปฏิบัติทางวิชาชีพ

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

↓ Markdown ↓ ข้อความธรรมดา ↓ PDF

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั่ง · SHA-256 5e32d8d0144f4d38a5df81a0caf03de29e155407b1f77eacf7820e2398cf3bc7

Cuadernos Lacre · **สิ่งพิมพ์ของ** Menzuri Gestión S.L. ·
เขียนโดย R.Eugenio · **เรียบเรียงโดยทีมงาน** Solo2

เว็บไซต์นี้ไม่ใช้คุกกี้ ทุกสิ่งที่เบราว์เซอร์ของคุณโหลดนั้นเราเป็นผู้เขียนหรือกำกับดูแล และโฮสต์อยู่บนเซิร์ฟเวอร์ยุโรปของเรา ได้แก่ ตัวนับการเข้าชมแบบไม่ระบุตัวตน (Umami โฮสต์เอง) และ JavaScript ขั้นต่ำที่จำเป็นสำหรับตัวเลือกภาษาและการตั้งค่าธีมสว่าง/มืดของคุณ ซึ่งจะถูกบันทึกไว้บนอุปกรณ์ของคุณเอง ไม่มีทรัพยากรจากบริษัทภายนอก ไม่มีเครื่องมือติดตาม ไม่มีการสร้างโปรไฟล์ ไม่มีการแชร์ข้อมูล หากคุณต้องการติดตามเรา: RSS