French CNIL Releases GDPR Compliance Toolkit

On March 15, 2017, the French data protection authority (CNIL) released its six step- GDPR compliance program together with GDPR-tailored templates for use by companies, the "GDPR Toolkit." The GDPR Toolkit is helpful for companies because it provides guidance that companies may directly include in their privacy programs. Companies with sophisticated privacy programs may also use the GDPR Toolkit as a reality check against CNIL and, more generally, European data protection authorities' standards and expectations for GDPR compliance.

Identify a privacy role	Map data flows	Prioritize actions	Carry out PIAs	Update policies, procedures and breach response	Keep records

Steps	CNIL's Recommendations	Documentation
1. Identify a privacy role	Appoint a data protection officer (DPO) as soon as possible, even in the absence of a legal requirement	DPO toolkit (in French): • https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees • https://www.cnil.fr/sites/default/files/typo/document/guide_pratique_prise_de_fonction_cil.pdf • https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees
2. Map the data flows	Prepare inventory of processing operations using CNIL's template	Data inventory template (in French): • https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles
3. Prioritize actions	On the basis of the inventory, prioritize actions in light of risk assessed. Important items pertain to: - Revision of notices for GDPR compliance - Information of processors on their new obligations - Technical implementation of rights of individuals - Security measures - Processing of sensitive data or of data of minors - Large–scale monitoring activities - Systematic evaluation of individual behavior, including profiling - Adequacy mechanism for international transfers	Security guidance, templates for vendor agreements, and cloud services are available (in French) at: • https://www.cnil.fr/sites/default/files/typo/document/guide_securite-vd.pdf • https://www.cnil.fr/sites/default/files/typo/document/20111027_mod_clause%20sous%20traitant_vd.pdf • https://www.cnil.fr/sites/default/files/typo/document/20111027_mod_clause%20confidentialite%20maintenance_vd.pdf
4. Carry out PIAs	Carry out privacy impact assessments (PIAs) before any new processing that is likely to result in high risks for the rights and freedoms of individuals	3 Guidelines for carrying out PIAs (in French): • https://www.cnil.fr/sites/default/files/typo/document/cnil-pia-1-methode.pdf • https://www.cnil.fr/sites/default/files/typo/document/cnil-pia-2-outillage.pdf • https://www.cnil.fr/sites/default/files/typo/document/cnil-pia-3-bonnespratiques.pdf
5. Update policies, procedures, and breach response	Prepare internal procedures to manage daily privacy matters, including: - Privacy team structure - Breach response plan - Individual rights requests and claims - Vendor management	New data breach notification form (in French): • https://www.cnil.fr/sites/default/files/typo/document/cnil_formulaire_notification_de_violations.pdf
6. Keep records	Demonstrate compliance with the GDPR through: - Data processing inventory - PIA records - Copies of transfer solutions implemented - Notices - Consent forms and evidence of consents - Procedures for the exercise of individual rights - Processor agreements - Breach response implemented	N/A