Consultation sur le projet de recommandation relative à l'authentification multifacteur

Synthèse des contributions

Le 31 mai 2024, la CNIL a lancé une consultation publique sur son projet de recommandation relative à l'authentification multifacteur afin de recueillir les difficultés d'interprétation suscitées par le texte. Les contributions ont nourri les travaux de la CNIL en vue de la publication de la recommandation.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Synthèse des contributions

Cette consultation publique a majoritairement fait l'objet de contributions de la part de professionnels de la sécurité des données et des systèmes d'information pouvant occuper différentes responsabilités, notamment DPO/DPD, RSSI, consultants et ingénieurs en cybersécurité ou responsables d'organismes.

À propos de la consultation publique de la CNIL sur le projet de recommandation MFA

La numérisation croissante de l'activité économique – y compris dans le secteur public – s'accompagne d'une nette augmentation des menaces cyber, qui se professionnalisent. Les solutions pour y faire face ont évolué pour une sécurité en profondeur basée sur des technologies mêlant intelligence artificielle, mutualisation et utilisation d'informations diverses, prise de décision automatisée, ou encore analyse du comportement des utilisateurs pour les plus avancées.

Ces solutions, comme l'authentification multifacteur, peuvent permettre de répondre notamment à l'obligation de sécurité des données (article 32 du règlement général sur la protection des données ou RGPD). Cependant, elles reposent elles-mêmes sur des traitements de données dont la conformité au RGPD doit aussi être assurée.

Afin d'accompagner les acteurs, la CNIL prévoit l'adoption d'une recommandation sur l'authentification multifacteur. Le but est de sécuriser les responsables de traitement – utilisateurs de telles solutions – et d'encourager les fournisseurs à adopter une approche de protection des données dès la conception.

Un projet de recommandation a été publié sur le site de la CNIL du 28 mars 2024 au 31 mai 2024 afin de recueillir les retours de l'écosystème. Ceux-ci ont été analysés et pris en compte lors de l'édition de la version finale de la recommandation.

Quelques chiffres sur les participants

18 contributions provenant de contributeurs issus de divers secteurs d'activité ont été reçues suite à la consultation : 3 administrations publiques, 4 éditeurs de solutions, 2 intégrateurs de solutions, 5 entreprises privées ou fédérations de professionnels, 2 associations de professionnels [paiement et SSI], 1 établissement public et 1 particulier. Parmi les participants, 4 étaient DPO, 7 avaient un poste lié à la sécurité des systèmes d'information et 7 avaient un poste de direction.

Les points clés des retours

Dans les grandes lignes, la diversité des avis lié à l'adéquation du périmètre, demandant souvent de traiter davantage de thématiques connexes (ex : *passkeys*, authentification par biométrie comportementale, authentification unique, identité numérique, etc.), démontre l'attente des responsables de traitements concernant une position doctrinale comme celle-ci notamment sur les solutions de cybersécurité. Les exemples pratiques sont appréciés de la plupart des participants.

Plusieurs participants ont indiqué que le projet de recommandation, de par sa structure inhabituelle, et certaines formulations prolixes, engendrait des difficultés de compréhension. Les thématiques transverses (ex : la biométrie, l'authentification multifacteur d'employés) abordées de façon complémentaire dans des sections distinctes ont été perçues comme une dispersion du propos difficile à appréhender. De plus, des répondants ont relevé des développements jugés trop longs sur les aspects relatifs au cadre juridique, pointant l'absence d'une posture claire sur des pratiques communes telle que l'usage du SMS OTP ou encore l'usage de l'équipement privé d'un employé comme facteur de possession.

Ces contributions ont permis à la CNIL :

- d'expliciter davantage le périmètre de la recommandation et de le recentrer sur l'objet de celle-ci : l'authentification multifacteur et sa conformité au RGPD ;
- de revoir la structure pour une meilleure lisibilité (en adoptant le plan classique d'une fiche de registre) ;
- de clarifier les principaux points incompris ;
- d'améliorer la recommandation en précisant certains des termes utilisés ;
- de formaliser une posture claire sur les pratiques communes remontées, sans préjuger du cadre sectoriel applicable.

Principales évolutions suite aux retours de la consultation

Sur le périmètre et sur les termes

- Modification de la définition du **facteur de possession** et clarification des solutions de **jeton logiciel** et **jeton matériel** associées
- Ajout d'un **encadré spécifique sur l'OTP SMS**
- Remplacement de l'encadré *Terminologie* par la nouvelle section ***2.3 Notions connexes à distinguer de l'authentification multifacteur*** visant à exclure du périmètre de la recommandation les méthodes d'authentification qui sont parfois confondues avec l'authentification multifacteur (tel que l'OTP par *email*).
- Formalisation de la nouvelle section 2.4 dédiée au périmètre de la recommandation. Fait notable par rapport à la version « projet » : la version finale de la recommandation met **hors périmètre la biométrie comportementale et biologique**. Par cohérence, les cas d'usages et développements associés à la biométrie comportementale ont été retirés. C'est notablement le cas de l'ancienne section *3.1 Vérifier si la mise en place d'une authentification multifacteur résulte d'une obligation légale* avec son encadré d'exemples de réglementations applicables, et l'encadré *Le cas particulier de l'usage additionnel de techniques basées sur les risques* de la section 3.3. Aussi, l'encadré *Le cas particulier de la biométrie morphologique* est réintégré dans le corps de la section car les autres biométries ne sont plus traitées.

Sur la structure et le fond

- Adoption d'un plan classique d'une fiche de registre :
  - Ajout des nouvelles sections :
    - *2.5 Données personnelles impliquées dans une authentification multifacteur*, à savoir les catégories de données personnelles concernées organisée selon le type de facteur d'authentification mobilisé ;
    - *2.6 Authentification multifacteur et RGPD*, à savoir la description du traitement et de ses finalités. La section permet également de clarifier la nature de l'authentification multifacteur : elle peut être considérée comme un traitement de données à caractère personnel mais également comme une mesure de sécurité.
  - Modification des sections 3.1 à 3.5 :
    - La section *3.1 Evaluer l'opportunité de mettre en place une authentification multifacteur* rationalise le contenu des anciennes sections *2.3 Pourquoi l'authentification multifacteur* et la fin de la section *3.2.1 Evaluer l'opportunité de mettre en place une authentification multifacteur*. Elle vise à inciter les responsables de traitement mettre en œuvre l'authentification multifacteur, quand le contexte le nécessite, et les questions à prendre en compte pour ce faire.

- La section 3.2 *Justifier d'une base légale pour le traitement d'authentification multifacteur* est une nouvelle version de l'ancienne section 3.2.2, distinguant davantage les sujets (nature du traitement - mesure de sécurité adossée à un traitement principal ou traitement en propre -, base légale et inscription au registre) afin de gagner en lisibilité. La description du cas de la base légale du contrat a été retirée. Les retours et la clarification associée ont permis de mettre en lumière le fait que, pour les personnes concernées, l'objet du contrat est le traitement principal reflétant le service (par exemple la fourniture d'une messagerie en ligne), l'authentification multifacteur étant une mesure de sécurité adossée. Par ailleurs, l'*exemple #1 Biométrie et consentement* a été remplacé par un encadré formalisant explicitement la position de la CNIL sur la question du ***Choix de la base légale et [en cas de] biométrie*** (retreinte à la biométrie morphologique, la biométrie comportementale et biologique étant hors périmètre) et un encadré sur l'encadré ***Choix de base légale dans le contexte professionnel*** a été ajouté**.**
- La section 3.3 *Choisir la solution en prenant en compte les risques relatifs aux personnes concernées* reprend en partie l'ancienne section 3.2.1 et les anciens exemple #4 et #5 (de la section 3.5) et restructure l'ancienne partie 3.3. L'objectif est de faire un focus sur les risques relatifs aux personnes selon la catégorie de facteur mobilisé et de présenter des cas pratiques répandus (OTP déverrouillée par code PIN, facteur biométrique et exemption domestique) avec les mesures de protection adéquates.
- La section 3.4 *Qualifier les acteurs et préciser leurs obligations* reste relativement similaire à l'ancienne version, modulo l'ajout de l'exemple *Une application OTP installée sur un terminal professionnel*
- La section 3.5 *Minimiser la collecte de données* est bien plus courte du fait du report de la description des données dans la nouvelle section 2.5 dédiée. Cette section est cependant mise à profit pour formaliser, en conjonction avec le nouvel encadré ***Choix de base légale dans le contexte professionnel*** de la section 3.2, la position de la CNIL sur l'articulation entre la base légale de l'intérêt légitime d'un employeur et le principe de minimisation dans le cas où une solution d'authentification multifacteur professionnelle ferait intervenir un équipement personnel de l'employé.

- Réorganisation et reformulations à la marge des trois dernières sections (3.6 à 3.9) en lien avec les évolutions sur les termes et à un travail lié à la rationalisation et distinction des thématiques entre elles.