IOTRUST

RÉFÉRENTIEL

MÉTHODOLOGIE IOTRUST

SOMMAIRE

LES ATTRIBUTIONS

LES AUTEURS

ANNE-LISE BOULET

Juriste au sein de la société Digitemis, **Anne-Lise BOULET** conseille et accompagne ses clients dans leur mise en conformité avec le règlement européen sur la protection des données personnelles (RGPD). Cet ouvrage aborde de manière pédagogique les principes juridiques à prendre en compte pour la conception d'objets connectés.

ADRIEN COUERON

Ingénieur en sécurité des systèmes d'information, **Adrien COUERON** a élaboré la structure de ce guide de bonnes pratiques en fonction des principaux manquements de sécurité constatés sur les objets étudiés dans le cadre du projet IoTrust.

ROMAIN GARNIER

Étudiant en Big Data et cloud computing à l'ESIEA, **Romain GARNIER** a rédigé ce guide dans le cadre de son « stage technique » au cours duquel il a travaillé sur une méthodologie d'audit d'objets connectés et particulièrement sur leurs applications Android.

LUDOVIC VALLY

Étudiant en système d'information à l'ESIEA, **Ludovic VALLY** a participé à la rédaction de ce guide en apportant ses réflexions et ses connaissances dans le domaine de l'IoT acquises au cours de son stage au laboratoire de sécurité informatique CNS.

2 PRÉSENTATION DES AUTEURS

SOUS LA SUPERVISION DE : RICHARD REY, DAVID CARNOT ET SLIM TOUHAMI

Richard REY : Ingénieur de recherche en sécurité informatique

David CARNOT : Consultant sécurité des systèmes d'information

Slim TOUHAMI : Juriste consultant RGPD / Vie privée

LE PROJET

FINALITÉS DU PROJET

Dans les années soixante-dix, les législations nationales, notamment française, se sont développées afin de limiter les atteintes aux données personnelles et, a fortiori, au respect de la vie privée des personnes. Avec le développement des nouveaux outils de communication et l'arrivée d'Internet, le transfert et l'exploitation des données personnelles ont été facilitées et la protection des données personnelles est devenue d'autant plus sensible.L'adoption, le 14 avril 2016, du règlement général européen sur la protection des données personnelles (RGPD) permet l'adaptation et l'harmonisation des outils juridiques aux nouveaux enjeux et risques de l'économie de la donnée.

Avec l'arrivée du règlement en mai 2018, les risques liés à la vie privée des personnes doivent désormais être pris en compte par le professionnel dès la conception (« privacy by design »), en passant par les phases de développement et de distribution des produits et services. Le principe de responsabilité (« accountability ») prévu par le règlement européen impose de démontrer la mise en place de mesures internes pour assurer la conformité à la législation sur la protection des données personnelles, et ce dès la conception du produit ou service.

Jusqu'à l'adoption du règlement, la labellisation d'un produit ou d'un service devait impérativement passer par la Commission Nationale de l'Informatique et des Libertés. Le législateur européen encourage désormais la certification d'organismes privés chargés de labelliser des procédures, des produits ou des services. Le projet IoTrust vise ainsi la création d'un organisme de certification en charge de vérifier et qualifier le niveau de conformité juridique et technique des objets connectés proposés par les industriels.

MÉTHODOLOGIE ET RÉFÉRENTIELS

Le référentiel comprend l'ensemble des exigences techniques et juridiques que l'objet ou le service doit satisfaire afin d'obtenir le label. Il vise à vérifier la sécurité des objets connectés et des flux de données, la gestion des données personnelles, et le respect de la législation, notamment des droits des utilisateurs.

| 1. LE COMITÉ DE PILOTAGE

Un comité de pilotage a défini un référentiel de labellisation, en prenant en compte les avis du consortium, composé de juristes, d'industriels du secteur de l'internet des objets, d'associations de protection de consommateurs et de spécialistes en sécurité de l'information.

| 2. L'OUTIL DE VALIDATION

Un outil de validation de la sécurité technique des objets connectés a également été développé à partir des référentiels de l'ANSSI, de l'OWASP (Open Web Application Security Project), du CEH (Certified Ethical Hacker) et de l'état de l'art des vulnérabilités. L'outil a vocation à analyser les flux de données transitant par l'objet pour en déterminer le niveau de sécurité.

| 3. LES TESTS PRÉLIMINAIRES

Des tests préliminaires ont ensuite été réalisés sur des objets connectés disponibles sur le marché et couvrant différents domaines de l'internet des objets (domotique, voiture connectée, bien-être…).

Le comité a enfin eu pour mission de rédiger le guide de bonnes pratiques à destination des concepteurs d'objets connectés.

| 4. LA CRÉATION DE L'ORGANISME

La création de l'organisme de labellisation est intervenue après finalisation du référentiel, de l'outil de validation de la sécurité technique et du guide de bonnes pratiques. Une demande de certification auprès de la CNIL a été déposée, permettant à l'organisme de délivrer un label européen, ayant force légale sur l'ensemble du territoire de l'Union européenne, pour une durée de trois ans.

DIFFÉRENTES PARTIES PRENANTES

La Fondation **MAIF**, reconnue d'utilité publique, finance la recherche dans le domaine de la prévention des risques qui affectent les personnes, les biens et la vie quotidienne. À l'image de sa participation au projet IoTrust, la fondation soutient des projets innovants dans le but de réduire les risques.

Digitemis accompagne ses clients dans la protection des données personnelles et dans la mise en place de politiques de cybersécurité. Elle propose également des prestations d'audit et de sensibilisation à la sécurisation des données ainsi que des formations et du conseil.

L'**ESIEA** (École supérieure d'informatique, électronique, automatique) forme des ingénieurs dans le domaine des sciences et technologies du numérique. L'ESIEA apporte son expertise dans le mise en place de solutions techniques innovantes pour la sécurisation des objets connectés.

0. ANALYSE INFORMATIONNELLE

Se placer dans le dossier **Preuves/0-Analyse informationnelle**.

INFORMATION PACKAGING

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est d'identifier les informations données aux consommateurs sur le produit et la gestion des données personnelles par l'application utilisateur.

DÉROULEMENT DE L'AUDIT

1 | Créer un dossier **0-Information packaging** qui contiendra l'ensemble des preuves pour ce point de contrôle

2 | Photographier toutes les faces de la boîte, réunir les photos dans un fichier docx et l'ajouter au dossier en la nommant **packaging.docx**

3 | Chercher les informations relatives à la technologie utilisée et les ajouter aux preuves en les nommant **technologie_utilisée.png**

4 | Chercher les informations relatives aux application(s) mobile(s) utilisé(s) et les ajouter aux preuves en les nommant **application_mobile.png**

5 | Chercher les informations relatives aux donnée(s) récolté(s) et les ajouter aux preuves en les nommant **donnée_collectée.png**

6 | Chercher toutes les autres informations pertinentes et les ajouter aux preuves en les nommant **type_information.png**

MENTIONS LÉGALES

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est d'identifier les informations données aux consommateurs sur le produit et la gestion des données personnelles par l'application utilisateur.

DÉROULEMENT DE L'AUDIT

1 | Créer un dossier **1-Mentions légales** qui contiendra l'ensemble des preuves pour ce point de contrôle

2 | Recenser tous les documents d'informations aux utilisateurs en créant un dossier pour chaque document et la nommant **nom_document{web, papier, application}**. Voici une liste non exhaustive :

A) Manuel utilisateur

B) Conditions générales de ventes

C) Conditions de confidentialité

D) Le contrat de licence de l'utilisateur final

3 | Chercher les informations relatives aux données personnelles envoyées sur chaque document, les reporter sur le référentiel en la nommant **données_personnelles{web, papier, application}**

4 | Chercher les informations relatives à la sécurité des données sur chaque document, les reporter sur le référentiel en la nommant **securité_données{web, papier, application}**

5 | Chercher les informations relatives aux transferts des données sur chaque document, les reporter sur le référentiel en la nommant **transferts_données{web, papier, application}**

6 | Chercher les informations relatives à la récupération et suppression des données sur chaque document, les reporter sur le référentiel en la nommant **recupération_suppression_donnée{web, papier, application}**

7 | Chercher les informations relatives à la conservation des données sur chaque document, les reporter sur le référentiel en la nommant **conservation_données{web, papier, application}**

8 | Chercher les informations relatives à la localisation des serveurs sur chaque document, les reporter sur le référentiel en la nommant **localisation_serveurs{web, papier, application}**

9 | Chercher les informations relatives à la création de compte sur chaque document, les reporter sur le référentiel en la nommant **creation_compte{web, papier, application}**

10 | Chercher les informations relatives à la suppression de compte sur chaque document, les reporter sur le référentiel en la nommant **suppression_compte{web, papier, application}**

1. DONNÉES COMMUNIQUÉES

Se placer dans le dossier **Preuves/1-Données communiquées.**

INTERCEPTION BLUETOOTH

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est d'analyser les communications entre le terminal utilisateur et le serveur distant mais aussi entre le terminal utilisateur et l'objet connectée pour obtenir le plus d'informations générales possible.

MÉTHODE EMPLOYÉE

Pour capturer des paquets Bluetooth LE sur Wireshark, il faut suivre les instructions suivantes :

Ouvrir un pipe en tapant la commande :

```
$ sudo mk_fo /tmp/pipe
```

Ouvrir Wireshark en tant que root sur le pipe :

```
$ sudo wireshark-k-i /tmp/pipe
```

Allez ensuite dans Edit -> Preferences -> Protocols -> DLT_USER -> Edit -> + -> « User 0 (DLT=147) » et saisir dans « Payload protocol » btle.

Sur un terminal, taper la commande pour commencer une capture Bluetooth LE :

```
$ sudo ubertooth-btle-f-c /tmp/pipe
```

DÉROULEMENT DE L'AUDIT

1 | Créer un dossier **1-Bluetooth**, un sous-dossier **Captures** qui contiendra l'ensemble des captures Wifi et un sous-dossier **Preuves** qui contiendra l'ensemble des preuves

2 | Réaliser les différentes captures au cours de l'utilisation de l'objet et de sa configuration. Ajouter les différentes captures faite dans le dossier **Captures** en les nommant **type_action.pcap** (exemple : allumer_éteindre_lampe.pcap)

3 | Ouvrir avec Wireshark les fichiers correspondants

4 | Regarder les protocoles de communications utilisés

5 | Si le protocole LE LL est utilisé, remplir le référentiel en indiquant le destinataire ainsi que la localisation et le protocole utilisé

6 | Si les données ne sont pas chiffrées, remplir le référentiel en indiquant les types de données qui sont en clair, le destinataire ainsi que la localisation et le protocole utilisé. Faire différentes captures d'écran et les ajouter dans le dossier **Preuves** en les nommant **information.png** (exemple : informations_lampe.png)

INTERCEPTION WIFI

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est d'analyser les communications entre le terminal utilisateur et le serveur distant mais aussi entre le terminal utilisateur et l'objet connectée pour obtenir le plus d'informations générales possible.

MÉTHODE EMPLOYÉE

L'installation terminée, il nous faut déterminer les adresses constructrices en jeu, c'est à dire celle de l'objet connectée et éventuellement celle de l'interface. Soit les données suivantes que nous utiliserons pour les captures :

- MAC_OC étant l'adresse constructeur de l'objet connecté. Il peut être déterminer soit sur l'objet connecté lui-même, soit dans la documentation technique fournie à l'utilisateur.
- MAC_INT étant l'adresse de l'interface (Smartphone/Tablette).
- INT étant l'interface de la plateforme de tests qui sera utilisé pour écouter les échanges (suivant la version de la distribution soit wlan0 ou wlp2s0).

Objet connecté accédant au cloud, interface non obligatoire

```
$ sudo tcpdump-nni INT-s 65535-w capture.pcap ether host MAC_OC
```

Objet connecté accédant directement au cloud et interagissant avec une interface

```
$ sudo tcpdump-nni INT-s 65535-w capture.pcap ether host MAC_INT
```

On trouvera les captures faites dans le dossier home de la machine.

DÉROULEMENT DE L'AUDIT

7 | Créer un dossier **1-Wifi**, un sous-dossier **Captures** qui contiendra l'ensemble des captures Wifi et un sous-dossier **Preuves** qui contiendra l'ensemble des preuves

8 | Réaliser les différentes captures au cours de l'utilisation de l'objet et de sa configuration. Ajouter les différentes captures faite dans le dossier **Captures** en les nommant **type_action.pcap** (exemple : allumer_éteindre_lampe.pcap)

9 | Ouvrir avec Wireshark les fichiers correspondants

10 | Regarder les protocoles de communications utilisés

11 | Si le protocole TLS est utilisé, lancer et configurer un proxy avec Burp. Aller dans l'onglet Target et utiliser l'objet pour lire les données communiquées. Reporter le type de données, les serveurs contactés ainsi que la localisation et le protocole utilisé dans le référentiel

12 | Si les données ne sont pas chiffrées, reporter les types de données qui sont en clair dans le champ destinataire ainsi que la localisation et le protocole utilisé. Faire différentes captures et les ajouter dans le dossier **Preuves** en les nommant **information.png** (exemple : informations_lampe.png)

2. CHIFFREMENT ET ENCODAGE

Se placer dans le dossier **Preuves/2-Chiffrement et encodage**.

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est de vérifier la sécurité mise en place au niveau des échanges, à savoir si le TLS/SSL est mis en place ou simplement si une communication TCP est utilisée pour le Wifi et aussi si le LE LL est mis en place ou simplement si une communication ATT est utilisée pour le Bluetooth.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir les captures sur le flux entre l'application et l'objet connectée

2 | Reportez oui s'il y a un protocole de chiffrement et la robustesse de celui-ci, sinon reportez non. Ajoutez la preuve au dossier en la nommant **chiffrement_application_objet.png**

3 | Ouvrir les captures sur le flux entre l'application et le serveur distant

4 | Reportez oui s'il y a un protocole de chiffrement et la robustesse de celui-ci sinon reportez non. Ajoutez la preuve au dossier en la nommant **chiffrement_application_serveur.png**

3. PERMISSIONS DE L'APPLICATION

Se placer dans le dossier **Preuves/3-Permissions de l'application**.

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est de vérifier les différentes permissions dont l'application mobile a besoin.

DÉROULEMENT DE L'AUDIT

1 | Créer un dossier **Android**, si une application Android existe :

A) Aller sur le Play Store-> Nom_Application-> Détails des autorisations

B) Lister les différentes permissions dont l'application à besoin, faire une ou plusieurs captures d'écran pour afficher toutes les permissions de l'application, les ajouter aux preuves en la nommant **permissions_android.png**

C) Pour chaque permission, reporter si elle est obligatoire et justifier l'utilisation de cette permission

2 | Créer un dossier **iOS**, si une application iOS existe :

A) Aller dans Réglages-> Nom_Application

B) Lister les différentes permissions dont l'application a besoin et faire une ou plusieurs captures d'écran pour afficher toutes les permissions de l'application, les ajouter aux preuves en la nommant **permissions_ios.png**

C) Pour chaque permission, reporter si elle est obligatoire et justifier l'utilisation de cette permission

4. GESTION ET STOCKAGE DES DONNÉES

Se placer dans le dossier **Preuves/4-Gestion et stockage des données**.

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est de vérifier, dans le cas d'une application mobile, si le stockage des données est sécurisé.

DÉROULEMENT DE L'AUDIT

1 | Dans le cas d'une application Android :

A) Utiliser **adb** pour récupérer les fichiers en lien avec l'application, suivre la suite des instructions (nécessite un téléphone rooté):

```
$ adb shell
# su
# cp-R /data/data/idApplication /storage/self/primary/
# exit
# exit
# adb pull /storage/self/primary/idApplication
```

B) Le moyen le plus simple d'obtenir l'**idApplication** est de faire une recherche de l'application sur play.google.com et de le chercher dans l'URL

Exemple: *https ://play.google.com/store/apps/details? id=com.nespresso.activities*

L'id de l'application Nespresso est **com.nespresso.activities**

C) Reporter tous les types de données dans le référentiel en indiquant si les données sont chiffrées ou pas, le type et la robustesse du chiffrement. Ajouter l'ensemble du dossier récupéré ainsi que les preuves dans le dossier

5. AUTHENTIFICATION

Se placer dans le dossier **Preuves/5-Authentification**.

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est de vérifier que la sécurité de la politique d'authentification au compte utilisateur.

DÉROULEMENT DE L'AUDIT

1 | Dans le cas d'une application mobile ou d'une interface web

A) Vérifier qu'il est possible de se créer un compte, si c'est le cas reporter oui et ajouter la preuve **creation_compte.png** au dossier

B) Vérifier qu'on est obligé de se connecter à l'application, si c'est le cas reporter oui et ajouter la preuve **connexion_obligatoire.png** au dossier

C) Vérifier la présence d'une politique de complexité de mot de passe en indiquant :

a - Le nombre de caractères minimum

b - Le nombre de catégories de caractères minimum parmi les 4 catégories suivantes :

i. Lettre majuscule

ii. Lettre minuscule

iii. Chiffre

iv. Caractères spéciaux

c - La possibilité de créer un mot de passe uniquement avec des chiffres

d- La possibilité de créer un mot de passe uniquement avec des minuscules

e - La possibilité de créer un mot de passe issu du dictionnaire

Reporter les différentes conditions du mot de passe et ajouter la preuve **politique_complexité_mdp** au dossier.

D) Vérifier qu'il est possible de récupérer son compte en cas de perte de mot de passe, si c'est le cas reporter oui et ajouter la preuve **recuperation_compte.png** au dossier

2 | Dans le cas où il y a l'application sous plusieurs OS, créer un dossier **Android** et un dossier **iOS**. Effectuer les points de contrôle suivant pour chaque OS

A) Vérifier qu'il est possible de se déconnecter du compte, si c'est le cas reporter oui et ajouter la preuve **deconnexion_compte.png** au dossier

B) Vérifier qu'un mécanisme anti brute force est en place et effectuant 11 connexions avec la bonne adresse email et un mauvais mot de passe puis une 12e fois avec le bon mot de passe. Reporter non si la connexion se réalise. Ajouter la preuve **anti_bruteforce.png** au dossier

6. PORTABILITÉ ET ACCÈS AU TYPES DE DONNÉES

Se placer dans le dossier **Preuves/6-Portabilité et accès au types de données**.

OBJECTIF DU POINT DE CONTRÔLE

L'objectif de ce point de contrôle est de vérifier si le droit à la portabilité est respecté.

DÉROULEMENT DE L'AUDIT

1 | Parcourir l'interface utilisateur, si elle donne la possibilité de télécharger les données personnelles de l'utilisateur. Enregistrer le fichier des données extraites et enregistrer le sous le nom **telecharger_données.ex**t (ext étant l'extension correspondant au type de fichier)

2 | Rechercher l'adresse de contact DPO/CIL du fabricant. Remplir le Template d'email **template_email_acces_donnees.docx**. Attendre les 2 mois réglementaires et ou la réponse du fabricant. Indiquer le délai de réponse et si la réponse est positive ou non. Faire une capture de l'email de réponse en la nommant **recuperation_données.png**

CONTOURNEMENT DU CERTIFICATE PINNING

Certaine application implémente une vérification des certificats utilisés pour initiés les communications avec les serveurs de l'éditeur. Dans ce cas, il n'est pas possible d'intercepter les communications et donc de vérifier la nature des échanges entre l'application et le serveur.

Il existe cependant une méthode permettant de contourner ces méthodes, en modifiant l'application mobile. Pour cela, il est nécessaire de :

1 | Récupérer et télécharger l'application au format binaire

2 | Décompiler l'application à l'aide de l'outil APKTool[1]

```
$./apktool d <PATH/TO/FILE.APK>
```

3 | Un dossier est alors créé avec le code source de l'application décompilé

4 | Identifier dans le code source la vérification du « certificat pinning »

A) Recherche les mots clefs « CheckClientTrusted » « CheckServerTrusted »

B) Rajouter la ligne « return-void » au début de la méthode (généralement après le .locals)

5 | Recompiler l'application via APKTool

```
$./apktool b <PATH/TO/APK/FOLDER> -o <FILE-MODIFIED.APK>
```

6 | Si nécessaire, signer l'APK :

A) Créer le keystore:

```
$ keytool -genkey -v -keystore iotrust.keystore -alias iotrust -keyalg RSA-keysize 248-validity 10000
```

B) Signer l'apk:

```
$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore iotrust.keystore <FILE-MODIFIED.APK> iotrust
```

L'application peut maintenant être installée.

[1] https://ibotpeaches.github.io/Apktool/install/

INTRODUCTION

OBJECTIF DE L'AUDIT : Déterminer si l'objet connecté est conforme au référentiel établi en matière de gestion des données personnelles. Ce référentiel s'appuie sur les principes fondamentaux du Règlement européen sur la protection des données à caractère personnel (RGPD).

Le référentiel juridique présente les différents points de contrôle à observer et la marche à suivre pour y parvenir.

En s'appuyant sur la documentation (conditions d'utilisation générale, contrat de licence, déclarations de confidentialité…) et les tests techniques réalisés, le résultat de l'audit indiquera le niveau de conformité de l'objet connecté.

1. RECENSEMENT ET CATÉGORISATION DES DONNÉES

OBJECTIF DU POINT DE CONTRÔLE

Recenser l'ensemble des données personnelles recueillies par l'objet et les catégoriser.

DÉROULEMENT DE L'AUDIT

1 | Copier le référentiel juridique nommé « 20180608_ALB_IoTrust_Référentiel_Juridique » (dossier Livrable D – Référentiel) dans le dossier de l'objet analysé.

2 | Ouvrir la page **Recensement des données** du référentiel juridique

3 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…)

4 | Dans la colonne « Données collectées selon la documentation », référencer toutes les données qui sont collectées selon la documentation

5 | Dans la première colonne « Type de données », catégoriser les données selon les choix proposés

Il est possible d'ajouter des lignes au tableau afin de correspondre au nombre exact de données collectées

6 | Ouvrir le dossier 1 – Données communiquées (ou le référentiel technique dans la page « Données communiquées ») contenant l'ensemble des données recueillies et constatées durant les analyses. Ouvrir le dossier 5 – Authentification permettant de vérifier quelles données sont collectées lors de la création d'un compte et l'utilisation de l'application

7 | Dans la colonne « Données collectées lors des analyses » référencer toutes les données qui sont collectées selon les analyses

8 | Dans la seconde colonne « Type de données », catégoriser les données selon les choix proposés

9 | Evaluer la conformité du point de contrôle en comparant les données issues des analyses à celles inscrites dans la documentation. Déterminer la concordance entre les deux en choisissant « Conforme » (si concordance) ou « Non conforme » (si pas de concordance) dans la colonne « Test de concordance »

2. DÉTERMINATION ET APPRÉCIATION DE LA FINALITÉ

OBJECTIF DU POINT DE CONTRÔLE

Vérifier la conformité des finalités.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Finalités** du référentiel juridique.

2 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…)

3 | A l'aide des documents, vérifier la présence de finalités. S'il existe une finalité, reporter un test concluant dans la case correspondante (**Présence de finalités**), à l'inverse reporter un test non concluant

4 | A l'aide de la documentation, vérifier que la finalité est :

A) Licite

B) Ethique

C) Corresponde à la fonction de l'objet connecté

Pour chacun des sous-points, reporter un test concluant ou non concluant dans la case correspondante en utilisant la légende proposée.

5 | L'évaluation de la légitimité de la finalité apparaît automatiquement dans la case **Conformité 1**

6 | A l'aide de la documentation, valider l'application du principe de minimisation des données en vérifiant que :

A) Les données collectées sont **pertinentes** vis-à-vis de la finalité annoncée

B) Les données collectées sont **proportionnées** vis-à-vis de la finalité annoncée

Pour chacun des sous-points, reporter un test concluant ou non concluant dans la case correspondante en utilisant la légende proposée.

7 | L'évaluation de la légitimité de la finalité apparait automatiquement dans la case **Conformité 2**

8 | L'évaluation de conformité du point de contrôle apparait automatiquement dans la case nommée « Evaluation »

3. VÉRIFICATION DE LA BASE LÉGALE

OBJECTIF DU POINT DE CONTRÔLE

S'assurer que le traitement repose sur une base légale.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Base légale** du référentiel juridique.

2 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…)

3 | Vérifier que les bases légales des traitements sont mentionnées dans la documentation. Indiquer si la preuve est présente ou absente dans la case correspondante (**Base légale mentionnée**) conformément à la légende proposée

4 | Si la base légale repose sur le consentement de l'utilisateur aller à l'étape 6. Si la base légale ne repose pas sur le consentement de l'utilisateur aller à l'étape 7.

5 | A l'aide de la documentation et des captures d'écran (dossier 5 – Authentification), vérifier la conformité du consentement en observant :

A) Le caractère **spécifique** du consentement

B) Le caractère **éclairé** du consentement

C) Le caractère **univoque** du consentement

D) Le caractère **libre** du consentement

Pour chacun des sous-points, reporter un test concluant ou non concluant dans la case correspondante en utilisant la légende proposée.

6 | Lorsque la base légale n'est pas le recueil du consentement de l'utilisateur, reporter un test « Non effectif » pour les cases correspondantes (**spécifique, éclairé, univoque, libre**)

7 | L'évaluation de conformité du point de contrôle apparait automatiquement dans la case nommée « Evaluation »

4. VÉRIFICATION DE L'EXISTENCE D'UNE DURÉE DE CONSERVATION

OBJECTIF DU POINT DE CONTRÔLE

Vérifier que les données ne sont pas conservées pour une durée illimitée.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Durées de conservation** du référentiel juridique

2 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…)

3 | A l'aide des documents disponibles, vérifier que les durées de conservation des données sont spécifiées

A) Si les durées de conservation sont spécifiées, reporter un test concluant

B) Si les durées de conservation ne sont pas spécifiées, reporter un test non concluant

4 | A l'aide des documents et en fonction des finalités, vérifier que les durées de conservation ne sont pas excessives.

A) Si les durées de conservation ne sont pas excessives, reporter un test concluant

B) Si les durées de conservation sont excessives, reporter un test non concluant

5 | L'évaluation de conformité du point de contrôle apparait automatiquement dans la case nommée « Evaluation »

5. DÉTERMINATION DU DESTINATAIRE DES DONNÉES ET TRANSFERT DE DONNÉES

OBJECTIF DU POINT DE CONTRÔLE

Contrôler la conformité des transferts de données hors Union Européenne.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Destinataires et transferts**

2 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…)

3 | A l'aide des documents, vérifier que **l'identité** du (des) destinataire(s) des données est transmise à l'utilisateur

A) Si l'information est transmise, reporter un test concluant dans la case correspondante

B) Si l'information n'est pas transmise, reporter un test non concluant

4 | A l'aide des documents, vérifier que la **localisation** du ou des destinataires des données est transmise à l'utilisateur

A) Si l'information est transmise, reporter un test concluant dans la case correspondante

B) Si l'information n'est pas transmise, reporter un test non concluant

5 | Ouvrir le référentiel technique

6 | Contrôler à la page **Données communiquées** du référentiel technique la présence de transferts de données personnelles hors union Européenne

A) En présence de transferts de données hors UE aller à l'étape 7

B) En l'absence de transfert de données hors UE aller à l'étape 11

7 | A l'aide de la documentation, vérifier que l'utilisateur a été **informé** de l'existence des transferts de données personnelles hors UE

A) Si l'information a été délivrée à l'utilisateur, reporter un test concluant à la case correspondante

B) Si l'information n'a pas été délivrée à l'utilisateur, reporter un test non concluant à la case correspondante

8 | A l'aide de la documentation, vérifier que le transfert de données repose sur une **base juridique**

A) Si le transfert repose sur une base juridique, reporter un test concluant à la case correspondante

B) Si le transfert ne repose pas sur une base juridique, reporter un test non concluant à la case correspondante

Préciser dans la case « Commentaires » sur quelle base juridique repose le transfert hors UE.

9 | A l'aide de la documentation, vérifier que les **finalités** du transfert de données sont précisées

A) Si les finalités sont précisées, reporter un test concluant à la case correspondante

B) Si les finalités ne sont pas précisées, reporter un test non concluant à la case correspondante

10 | A l'aide de la documentation, vérifier que les finalités du transfert de données sont **légitimes**

A) Si les finalités sont légitimes, reporter un test concluant à la case correspondante

B) Si les finalités ne sont pas légitimes, reporter un test non concluant à la case correspondante

11 | L'évaluation de conformité du point de contrôle apparait automatiquement dans la case nommée « Evaluation »

6. SÉCURITÉ DES RÈGLES D'AUTHENTIFICATION

OBJECTIF DU POINT DE CONTRÔLE

Contrôler le niveau de sécurité des règles d'authentification.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Authentification** du référentiel juridique

2 | Ouvrir le référentiel technique

3 | Vérifier qu'un mot de passe suffisamment complexe est nécessaire pour utiliser l'objet connecté. Pour cela, s'appuyer sur la page **5 - Authentification** du référentiel technique

Si la politique de mots de passe est suffisamment complexe, reporter un test concluant dans la case correspondante du référentiel juridique.

Si la politique de mots de passe n'est pas assez complexe, reporter un test non-concluant dans la case correspondante du référentiel juridique.

4 | Vérifier qu'il est possible de se déconnecter de son compte utilisateur en s'appuyant sur la page **5 – Authentification** du référentiel technique

S'il est possible de se déconnecter de son compte utilisateur, reporter un test concluant dans la case correspondante dans le référentiel juridique.

S'il n'est pas possible de se déconnecter de son compte utilisateur, reporter un test non-concluant dans la case correspondante dans le référentiel juridique.

5 | Vérifier à la page **5 - Authentification** du référentiel technique qu'un mécanisme anti brute-force est mis en place

Si la référence présente un test concluant, reporter un test concluant à la case correspondante du référentiel juridique.

Si la référence présente un test non-concluant ou non-effectif, reporter un test non-concluant ou non-effectif à la case correspondante du référentiel juridique.

7. INFORMATION DES PERSONNES ET EXERCICE DES DROITS

OBJECTIF DU POINT DE CONTRÔLE

Vérifier que les utilisateurs ont bien reçues les informations obligatoires et qu'ils peuvent exercer leurs droits.

DÉROULEMENT DE L'AUDIT

1 | Ouvrir la page **Information et droits**.

2 | Ouvrir les dossiers Technique/Preuves/0-Phase préliminaire contenant l'ensemble de la documentation existante pour l'objet connecté (politique de confidentialité, conditions générales d'utilisation, notice d'utilisation…) et le référentiel technique.

3 | Vérifier à l'aide de l'ensemble des documents que les informations suivantes ont bien été transmises à l'utilisateur (**Information de l'utilisateur**) :

A) L'identité et les coordonnées du responsable de traitement

B) Les coordonnées du délégué à la protection des données ou du correspondant informatique et libertés *(S'il n'y en a pas, reporter un test non effectif)*

C) Les finalités du traitement

D) Le ou les destinataires des données

E) La réalisation de transfert de données hors Union Européenne

F) Les durées de conservation des données

G) La procédure d'exercice du droit de rectification

H) La procédure d'exercice du droit d'opposition

I) La procédure d'exercice du droit à la limitation

J) La procédure d'exercice du droit de suppression

K) La procédure d'exercice du droit à la portabilité

L) La possibilité de retirer son consentement à tout moment

Pour chacun des sous-points, reporter un test concluant ou non concluant dans la case correspondante en utilisant la légende proposée.

4 | Vérifier à l'aide des documents que l'utilisateur est informé de son **droit d'accès**.

A) S'il en est informé, reporter un test concluant à la case correspondante

B) S'il n'en est pas informé, reporter un test non concluant à la case correspondante

5 | Ouvrir la page **6 – Récupération données perso** du référentiel technique. A l'aide de ce document, vérifier que le droit d'accès est effectif.

A) Si le droit d'accès est effectif, reporter un test concluant à la case correspondante

B) Si le droit d'accès n'est pas effectif, reporter un test non-concluant à la case correspondante.

6 | L'évaluation du point de contrôle apparaît automatiquement.

7 | Vérifier que la documentation précise la possibilité pour l'utilisateur de supprimer ses données (**droit de suppression**).

A) Si la documentation le précise, reporter un test concluant à la case correspondante

B) Si la documentation ne le précise pas, reporter un test non effectif à la case correspondante

8 | Vérifier à la page **5 – Authentification** du référentiel technique que l'utilisateur a réellement la capacité de supprimer les données collectées par lui-même.

A) S'il est possible de supprimer les données lui-même, reporter un test concluant

B) S'il n'est pas possible de supprimer les données lui-même, reporter un test non concluant

9 | L'évaluation du point de contrôle apparaît automatiquement.

10 | Vérifier que la documentation précise la possibilité pour l'utilisateur d'exercer son **droit de portabilité**.

A) Si la documentation le précise, reporter un test concluant à la case correspondante

B) Si la documentation ne le précise pas, reporter un test non effectif à la case correspondante

11 | Vérifier à l'aide de la page **6 – Récupération données perso** du référentiel technique que l'utilisateur a réellement la capacité d'exporter ses données collectées.

A) S'il est possible d'exporter ses données, reporter un test concluant à la case correspondante

B) S'il n'est pas possible d'exporter ses données, reporter un test non concluant

12 | Vérifier que l'export des données est réalisé dans un format :

A) Structuré

B) Couramment utilisé

C) Lisible par machine

13 | L'évaluation de conformité du point de contrôle apparait automatiquement dans la case nommée « Evaluation ».

Un projet soutenu par la fondation MAIF.

Graphiste : Betty Bulleux
Responsable Projet : Slim Touhami
Responsable Communication : François Guibert

Réalisé en **Juin 2018**

DIGITEMIS
CYBERSECURITY & PRIVACY

IOTRUST