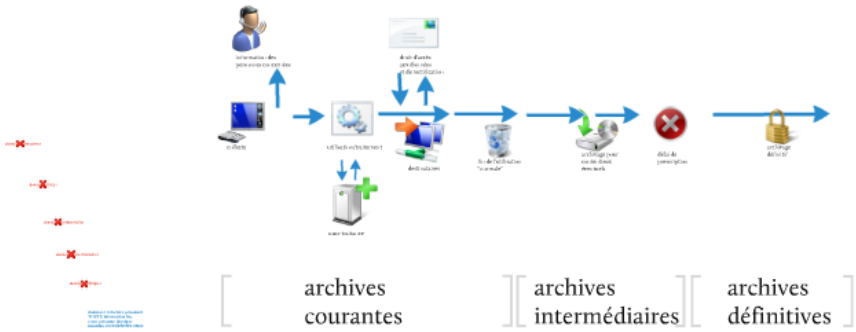
Cycle de vie des données à caractère personnel



en résumé:
- le MOA m'a-t-il bien précisé sa finalité?
- le contenu du traitement est-il bien proportionné à la finalité?
- ai-je prévu le délai en cas de demande d'autorisation à la CNIL?
- mes SI sont-ils bien sécurisés?
- quel est le processus d'information des personnes concernées (y.c. IRP)?
- ai-je une clause adaptée dans mes marchés de sous-traitance?
- comment sont gérées les habilitations?
- comment s'exercera le droit d'accès?
- comment sont gérés la durée de conservation et l'effacement?
- le MOA a-t-il besoin d'archives intermédiaires?
- le MOA a-t-il besoin d'archives définitives, et sous quel format?

Cycle de vie des données à caractère personnel

Dominique Chaumet **5 mai 2011** GROUPE RATP

données nominatives

données  confidentielles

données professionnelles

données publiques

données à caractère personnel:
TOUTE information liée
à une personne physique
identifiée OU IDENTIFIABLE

collecte

utilisation

effacement

collecte → utilisation → effacement

collecte → utilisation → effacement

collecte → utilisation → effacement

collecte → utilisation → effacement

traitement des données

données à caractère personnel:
TOUTE information liée
à une personne physique
identifiée OU IDENTIFIABLE

archives
courantes

procédure préalable I & L

collecte → utilisation → effacement

collecte → utilisation → effacement

collecte → utilisation → effacement

collecte → utilisation → effacement

traitement des données

sécurisation

formalités

procédure préalable I & L

formalités

simple déclaration

demande d'autorisation à la CNIL

- numéro de sécurité sociale
- transfert hors U.E.
- données génétiques
- données relatives aux infractions
- traitements pouvant aboutir à l'exclusion du bénéfice d'un droit
- biométrie
- appréciation des difficultés sociales
- recherche dans le domaine de la santé
- sûreté de l'État

sécurisation

ANALYSER LES RISQUES
- Recenser les données à caractère personnel et les traitements
- Déterminer les menaces et leurs impacts sur la vie privée des personnes
- Mettre en œuvre des mesures de sécurité adaptées aux menaces

AUTHENTIFIER LES UTILISATEURS
- Définir un identifiant (login) unique à chaque utilisateur
- Adopter une politique de mot de passe utilisateur rigoureuse
- Obliger l'utilisateur à changer son mot de passe après réinitialisation

GÉRER LES HABILITATIONS ET SENSIBILISER LES UTILISATEURS
- Définir des profils d'habilitation
- Supprimer les permissions d'accès obsolètes
- Documenter les procédures d'exploitation
- Rédiger une charte informatique et l'annexer au règlement intérieur

SÉCURISER LES POSTES DE TRAVAIL
- Limiter le nombre de tentatives d'accès à un compte
- Installer un "pare-feu" (firewall) logiciel
- Utiliser des anti-virus régulièrement mis à jour
- Prévoir une procédure de verrouillage automatique de session

SÉCURISER L'INFORMATIQUE MOBILE
- Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage mobiles (clés USB, CD, DVD...)

SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ
- Effectuer des sauvegardes régulières
- Stocker les supports de sauvegarde dans un endroit sûr
- Prévoir des moyens de sécurité pour le convoyage des sauvegardes
- Prévoir et tester régulièrement la continuité d'activité

ENCADRER LA MAINTENANCE
- Enregistrer les interventions de maintenance dans une main courante
- Effacer les données de tout matériel avant sa mise au rebut
- Recueillir l'accord de l'utilisateur avant toute intervention sur son poste

TRACER LES ACCÈS ET GÉRER LES INCIDENTS
- Prévoir un système de journalisation
- Informer les utilisateurs de la mise en place du système de journalisation
- Protéger les équipements de journalisation et les informations journalisées
- Notifier les personnes concernées des accès frauduleux à leurs données

PROTÉGER LES LOCAUX
- Restreindre les accès aux locaux au moyen de portes verrouillées
- Installer des alarmes anti-intrusion et les vérifier périodiquement

PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE
- Limiter les flux réseau au strict nécessaire
- Sécuriser les accès distants des appareils informatiques nomades par VPN
- Utiliser le protocole SSL avec une clé de 128 bits pour les services web
- Mettre en œuvre le protocole WPA-AES/CCMP pour les réseaux WiFi

SÉCURISER LES SERVEURS ET LES APPLICATIONS
- Adopter une politique de mot de passe administrateur rigoureuse
- Installer sans délai les mises à jour critiques
- Assurer une disponibilité des données

GÉRER LA SOUS-TRAITANCE
- Prévoir une clause spécifique dans les contrats des sous-traitants
- S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites...)
- Prévoir les conditions de restitution et de destruction des données

ARCHIVER
- Mettre en œuvre les modalités d'accès spécifiques aux données archivées
- Détruire les archives obsolètes de manière sécurisée

SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES
- Chiffrer les données avant leur envoi
- S'assurer qu'il s'agit du bon destinataire
- Transmettre la clé de déchiffrage par envoi distinct et via un canal différent

information des
personnes conce

collecte

information des
personnes concernées

collecte

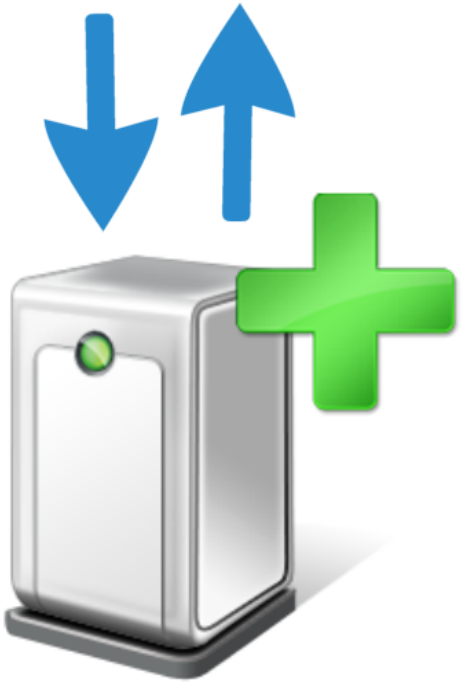
information des
personnes concernées

collecte

utilisation/traitement

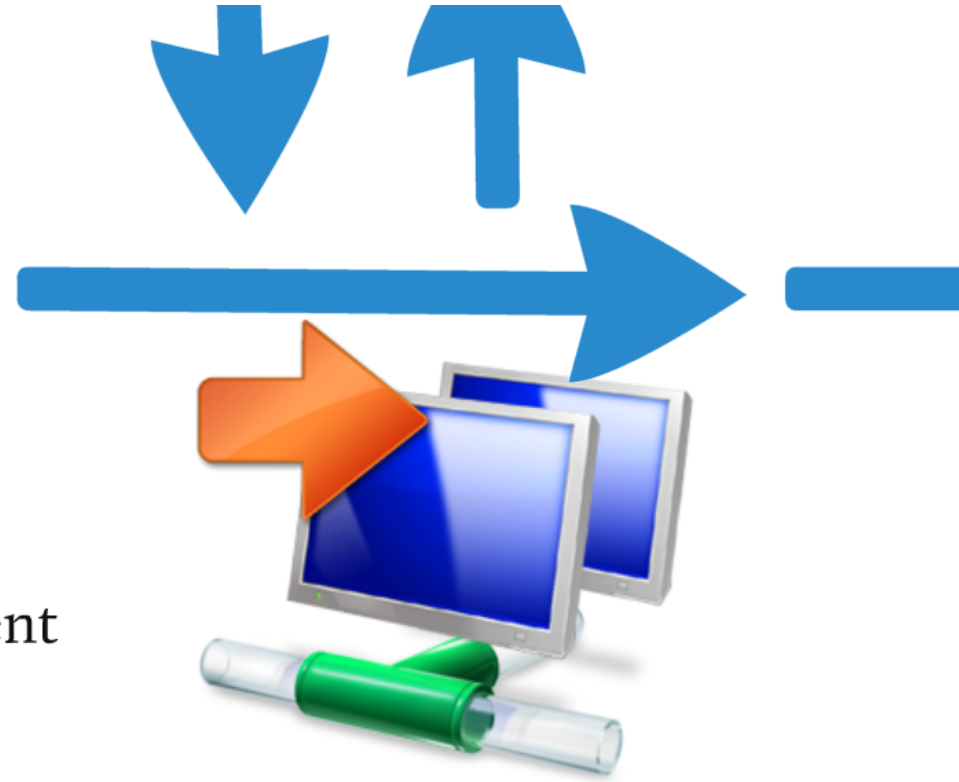
collecte

utilisation/traitement

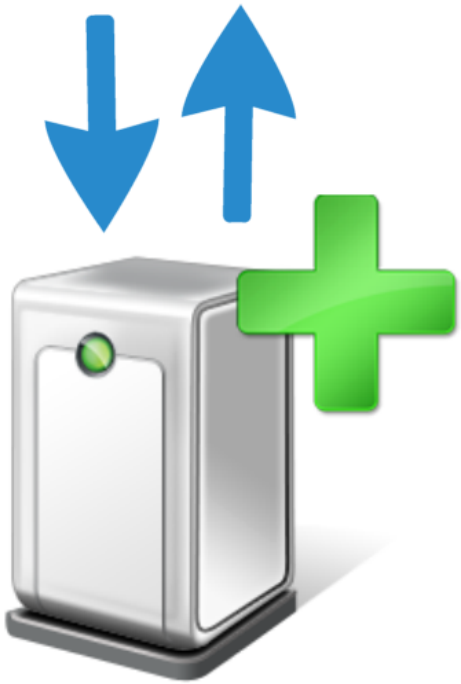


sous-traitance

utilisation/traitement



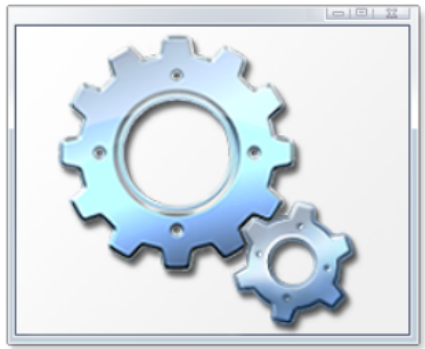
destinataires



sous-traitance

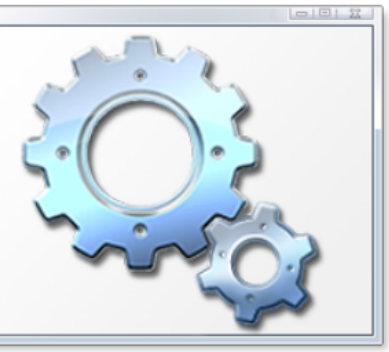
on des
concernées

droit d'accès
aux données
et de rectification



utilisation/traitement

droit d'accès
aux données
et de rectification



lisation/traitement

destinataires

fin de l'utilisation
"normale"

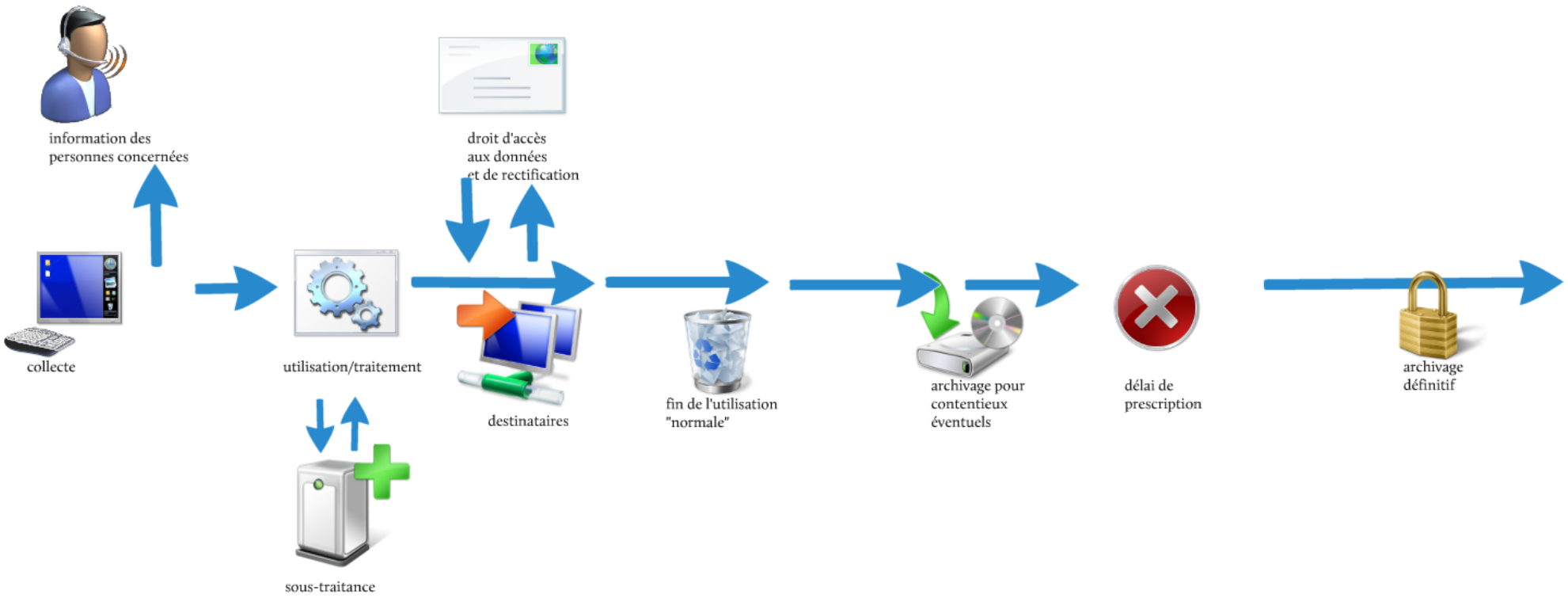
'utilisation
ale"

archivage pour
contentieux
éventuels

délai de
prescription

délai de
prescription

archivage
définitif



[archives courantes][archives intermédiaires][archives définitives]

en résumé:
- le MOA m'a-t-il bien précisé sa finalité?
- le contenu du traitement est-il bien proportionné à la finalité?
- ai-je prévu le délai en cas de demande d'autorisation à la CNIL?
- mes SI sont-ils bien sécurisés?
- quel est le processus d'information des personnes concernées (y.c. IRP)?
- ai-je une clause adaptée dans mes marchés de sous-traitance?
- comment sont gérées les habilitations?
- comment s'exercera le droit d'accès?
- comment sont gérés la durée de conservation et l'effacement?
- le MOA a-t-il besoin d'archives intermédiaires?
- le MOA a-t-il besoin d'archives définitives, et sous quel format?