Ministère de la culture

Examen professionnalisé réservé de secrétaire administratif des administrations de l'Etat affecté au traitement de l'information en qualité de programmeur (loi Sauvadet), session 2018

Mardi 30 octobre 2018

Épreuve écrite d'admissibilité : langage choisi PHP

18-DEC4-07059

Établissement de l'algorithme (sous forme d'ordinogramme) correspondant à la solution d'un problème simple et écriture des séquences de programme demandées correspondantes. La programmation devra être réalisée dans un langage évolué choisi par le candidat sur une liste fixée par arrêté du ministre ou de l'autorité d'accueil.
(durée : trois heures ; coefficient : 2).

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

- L'usage de la calculatrice, d'un dictionnaire ou de tout autre document est interdit.

- Le candidat ne doit faire apparaître aucun signe distinctif dans sa copie, ni son nom ou un nom fictif, ni signature ou paraphe.

- Seul l'usage d'un stylo noir ou bleu est autorisé (bille, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.

- Le candidat doit rédiger sa copie dans une seule et même couleur (bleu ou noir) : tout changement de couleur dans sa copie est considéré comme signe distinctif.

- Les feuilles de brouillon ou tout autre document ne sont pas considérés comme faisant partie de la copie et ne feront par conséquent pas l'objet d'une correction.

Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

 Le candidat devra rendre avec sa copie la page n°13 de ce sujet.

Ce document comporte 13 pages au total :

- Page de garde (1 page)
- Sujet (3 pages : 2 à 3 et 13)
- Annexes (9 pages) :
    * Annexe n°1 (7 pages : pages 4 à 10)
    * Annexe n°2 (2 pages : pages 11 et 12)

Ministère de la culture

Examen professionnalisé réservé de secrétaire administratif des administrations de l'Etat affecté au traitement de l'information en qualité de programmeur (loi Sauvadet), session 2018

Mardi 30 octobre 2018

Épreuve écrite d'admissibilité : langage choisi PHP

ÉTUDE DE CAS

CONTEXTE

Dans le cadre de la mise en place du règlement général de la protection des données, les établissements comme les entreprises doivent tenir à jour un registre de tous les traitements concernant des données à caractère personnel. Ce règlement contient 99 articles, nous allons dans le cadre de ce travail s'intéresser à l'article 30 fourni en annexe n°2.

Dans cet article, l'autorité exige la tenue d'un registre dans lequel sont renseignés les différents traitements procédés par l'établissement ou ses sous-traitants.

Nous partons du principe qu'on vous a sollicité(e) pour réaliser un prototype de registre qui permet d'enregistrer des processus de traitements existants ou à venir, cet outil va être installé dans un premier temps sur le poste de travail de la personne désignée comme délégué à la protection des données. Il sera amélioré par la suite selon les usages qu'on en fait.

Cette IHM (Interface Homme-Machine), en oubliant les aspects graphiques, sera réalisée en langage PHP.

TRAVAIL À RÉALISER

1) Avant d'intervenir sur le code de l'IHM, donnez la liste **des propriétés et leur type** associé sur le diagramme de classes UML (langage de modélisation unifié, de l'anglais Unified Modeling Language), représentant une possibilité de réalisation de ce registre en vous reportant à **l'annexe n°1**. Pour cela, vous devez compléter sur le diagramme de classes situé page 13 (à rendre avec la copie) les cases « Registre », « Activite » et Securite ».

2) Complétez (page 13/13) les trois cardinalités manquantes **dans** les symboles rectangulaires (☐) sur le diagramme de classes (page 13/13) **ou à côté** de ces symboles rectangulaires (☐).

3) Écrire le code PHP de la classe :

a. Activite

b. Registre

4) Proposer une solution pour intégrer les mesures de sécurité à notre prototype.

5) Modifier le code de la classe « **Activite** » pour prendre en compte un ou plusieurs responsables conjoints du traitement. **(Voir annexe n°2).**

6) Écrire en pseudo-code ou en PHP l'algorithme qui permet d'ajouter un élément dans un tableau seulement s'il n'existe pas. On pourra par exemple s'inspirer d'un tableau de catégories de personnes « catpersonnes ».

7) Pourquoi dit-on généralement que le langage PHP est un langage faiblement typé ? Vous pouvez argumenter par l'exemple.

8) Expliquez ce que pourrait faire ce code.

```
<?php

if(intval($_GET['id'])){

        $id = $_GET['id'];

        $registre = new Registre;

        $registre->afficher($id);

} else {

        Echo 'Rien à afficher' ;

}

?>
```

9) Le code ci-dessous initialise la variable personnes. Écrire le code qui permettra l'affichage à l'écran suivant :
Jasmine Grandiossa : 0611121314
Sara Boucle : 0708091011
Ambre Piccola : 0607080910

```
<?php

$personnes=array(
1 => array('prenom' => 'Jasmine', 'nom' => 'Grandiossa', 'telephone' => '0611121314'),
2 => array('prenom' => 'Sara', 'nom' => 'Boucle', 'telephone' => '0708091011'),
3 => array('prenom' => 'Ambre', 'nom' => 'Piccola', 'telephone' => '0607080910')
);

<Code à écrire>

?>
```

ANNEXES

Annexe n°1 : exemple de registre

Pour faciliter la tenue du registre, la commission nationale de l'informatique et des libertés de France (CNIL) propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme **en tant que responsable de traitement**. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévu par le règlement général sur la protection des données (RGPD).

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la règlementation.

Composition du document :

1. Une première page du registre recense les informations communes à toutes vos activités de traitement :
   - les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
   - les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
   - la liste des activités de votre organisme impliquant le traitement de données personnelles.

2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.
   Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.

Registre des activités de traitement de [Nom de l'organisme]

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	*Ex : NOM prénom du responsable légal* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	*Ex : NOM prénom du DPO* *Société (si DPO externe)* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Gestion de la paie*
Activité 2	*Gestion des prospects*
Activité 3	*Gestion des fournisseurs*
Activité 4	*Vente en ligne*
Activité 5	*Sécurisation des locaux*
Activité 6	
Activité 7	
Activité 8	
Activité 9	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

_____

_____

_____

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. _____
2. _____
3. _____

Catégories de données collectées

Listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

_____

☐ Vie personnelle *(habitudes de vie, situation familiale, etc.)*

_____

☐ Vie professionnelle *(CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

_____

☐ Informations d'ordre économique et financier *(revenus, situation financière, données bancaires, etc.)*

_____

☐ Données de connexion *(adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*

_____

☐ Données de localisation *(déplacements, données GPS, GSM, ...)*

_____
_____

☐ Internet *(cookies, traceurs, données de navigation, mesures d'audience, ...)*

_____

☐ Autres catégories de données *(précisez)* :

_____

_____

_____

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? :

_____

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ? (jours, mois ou ans ou autre durée)

_____

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

_____

_____

_____

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. _____
2. _____
3. _____
4. _____

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. _____
2. _____
3. _____
4. _____

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. _____
2. _____
3. _____
4. _____

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays :

_____

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs. Décrivez les mesures :

_____

_____

_____

☐ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

_____

_____

_____

☐ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

_____

_____

_____

☐ Sauvegarde des données. Décrivez les modalités :

_____

_____

_____

☐ Chiffrement des données

Décrivez les mesures (e*xemple : site accessible en https, utilisation de TLS, etc.)* :

☐ Contrôle des sous-traitants Décrivez les modalités :

☐ Autres mesures :

Annexe n°2 : Extrait du règlement général sur la protection des données

Article 30 - Registre des activités de traitement

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

   a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

   b) les finalités du traitement ;

   c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

   d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

   e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

   f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

   g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

   a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

   b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

   c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

   d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

4. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

<u>À rendre avec la copie</u>

Diagramme de classes