privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Guide pour les portails web de l'administration publique

1 Introduction

Les nouvelles technologies offrent la possibilité de mettre à disposition et d'utiliser des services 24 heures sur 24. Celui qui veut bénéficier durablement de la digitalisation doit en permanence évaluer les risques, et prendre des mesures de sécurité. Le présent guide est consacré aux exigences juridiques et techniques des portails web de l'administration publique. Il soutient les organes publics dans la planification et l'exploitation de tels portails web, offre des repères à leur développement et sert à leur l'évaluation par les préposés à la protection des données.

2 Notions

Identification/Vérification/Authentification/Autorisation: En pratique, il y a souvent confusion dans l'utilisation de ces notions. Dès lors qu'il n'existe pas de définition communément admise, ces notions seront définies et distinguées l'une de l'autre.

Ainsi, les notions les plus importantes suivantes sont décrites ci-après:

Notion	Description
Identification officielle	Une identification officielle permet de confirmer, sur un plan juridique, l'identité d'une personne sur la base d'un processus administratif mis en œuvre par une institution autorisée. Exemples de processus administratifs: • Passage personnel au guichet d'une administration • Identification au moyen d'une lettre • Un tiers fait un contrôle au moyen d'une pièce d'identité officielle (p.ex. Suisse ID ou Mobile ID) En principe, la preuve de l'identité ne devrait être requise que dans les cas où c'est nécessaire pour l'opération ou la prestation requise.
Vérification liée à un attribut	Par la vérification liée à un attribut d'une utilisatrice ou d'un utilisateur, on contrôle un élément appartement à cette personne. Par exemple, on vérifie si un code de confirmation (transmis par SMS) a été reçu au numéro de téléphone portable indiqué à cet effet. Autres exemples: • Vérification d'une adresse E-Mail • Confirmation du numéro de téléphone
Authentification (Authentication = processus de vérification)	Avec une authentification, on contrôle si les informations d'inscription d'une utilisatrice ou d'un utilisateur sont correctes (souvent: nom d'utilisatrice/utilisateur et mot de passe) et correspondent aux données enregistrées dans le système.
Autorisation (Authorization)	L'autorisation a pour objet d'attribuer des droits spécifiques à une personne. Après une authentification réussie, l'utilisatrice ou l'utilisateur ne peut pas automatiquement bénéficier des services ou des prestations déterminés. C'est l'autorisation qui déterminera la portée exacte des droits attribués. En revanche, l'autorisation suppose une authentification préalable et réussie.

Notion	Description
Portail	Le portail désigne un point d'accès disponible sur internet (Single Point of Access) afin que les utilisatrices et utilisateurs puissent accéder aux services et aux opérations mis à disposition par des organes publics (autorités de niveau communal, cantonal ou fédéral).
Enregistrement	L'enregistrement est la première inscription d'une habitante ou d'un habitant pour obtenir un compte ou un service offert par le portail. Selon l'opération ou la prestation souhaitée, une vérification liée à un attribut suffit ou alors il faut une identification officielle.

Tableau 1: Notions

3 Types de portails

En principe, on distingue entre un portail de passage et un portail de données de base.

Un portail de passage sert exclusivement à l'authentification et à l'autorisation de l'utilisatrice ou l'utilisateur, avant que celle-ci ou celui-ci puisse accéder à une application spécialisée. Ce portail n'enregistre donc que les données d'authentification ou d'autorisation.

Les données d'authentification et d'autorisation enregistrées dans le portail de passage sont par exemple:
- Nom d'utilisatrice/utilisateur et mot de passe
- Informations liées à n-facteurs
  - Numéro du téléphone mobile/certificat de signature électronique selon les SCSE
  - etc.
- Informations liées à l'autorisation et aux droits attribués
  - Autorisations d'accès à des applications spécialisées
  - Procurations et droits d'accès
- Si et comment une utilisatrice ou un utilisateur ont été identifiés
- Informations sur le statut

Dans un portail de données de base, les données liées à l'authentification et l'autorisation sont aussi enregistrées (voir ci-dessus, pour le portail de passage). Les données de base sont, en plus, enregistrées respectivement importées d'autres applications spécialisées. Les données de base peuvent aussi être exportées dans des applications spécialisées.

Les données de base sont:
- Prénom, nom et adresse
- Langue de correspondance
- Réglage du portail
- etc.

Il peut arriver, en pratique, que pour certaines applications spécialisées d'un portail de données de base, aucune donnée de base ne soit enregistrée, mais seulement les données d'authentification et d'autorisation.

Selon l'opération en question, il est possible que le portail enregistre, en plus et de manière temporaire ou permanente, des données de l'application spécialisée. Dans un tel cas, les exigences liées au portail et à l'application spécialisée sont identiques.

4 Exigences liées à l'enregistrement d'une utilisatrice ou d'un utilisateur

Les exigences liées à l'enregistrement et à l'éventuelle identification qui en découle dépendent de l'opération concrète envisagée, des données à traiter et des exigences spécifiques de l'application spécialisée. Ces exigences doivent être vérifiées dans chaque cas concret.

En cas d'enregistrement d'une Newsletter par SMS, une vérification de l'attribut „numéro de téléphone" peut, selon les circonstances, être suffisante. Pour des opérations plus complexes et pour le traitement de données sensibles, on exigera, dans certains cas, une identification officielle.

Le tableau suivant comporte certains exemples pour l'enregistrement pouvant s'opérer par vérification d'un attribut et par une identification officielle.

Vérification/Identification	**Cas d'application pour l'enregistrement**
Vérification liée à un attribut	• Inscription pour une Newsletter par E-Mail • Rappel SMS pour le calendrier d'élimination des déchets • …
Identification officielle	• Déclaration fiscale online • Demande d'une bourse d'étude • …

Tableau 2: Cas d'application pour l'enregistrement

5 Exigences liées à l'authentification d'une utilisatrice ou d'un utilisateur

Les exigences concrètes et les mesures liées à l'authentification dépendent de l'opération concrète envisagée, des données à traiter et des exigences spécifiques de l'application spécialisée. L'authentification ne signifie pas toujours qu'un nom d'utilisatrice/utilisateur ou un mot de passe soient exigés pour l'accès. Selon les circonstances, il peut suffire de rendre plausible les informations (comparaison avec des dates actuelles détenues par les autorités communales ou cantonales). Si des prestations offertes par le même portail exigent une authentification différente (p.ex. une authentification faible dans un cas et une authentification forte dans l'autre), on peut ou bien exiger dès le début l'authentification forte ou alors ne demander les critères de l'authentification forte qu'au moment où le service correspondant est souhaité.

Le tableau suivant énumère des cas d'authentification et les classifie.

Authentification	**Description**
Simple:	• Applicable pour des cas avec des données personnelles • Nom de l'utilisatrice/utilisateur et mot de passe • Rendre plausible des données personnelles avec des données actuelles dont on dispose (p.ex. no de série du véhicule, adresse de domicile ou date d'anniversaire)

Authentification	Description
Forte: 2-facteurs n-facteurs	Applicable pour des cas avec des données personnelles sensibles: • Smartcard/certificat • TAN/mTAN/One-time Password (OTP) • Un tiers prestataire vérifie avec un login à deux facteurs (p.ex. Mobile ID) • Vérification et confirmation par app • … • Dans certains cas (traitement de données sensibles) une authentification avec n-facteurs (3 facteurs ou plus) est nécessaire. Il faut vérifier cela dans les cas concrets.

Tableau 3: Résumé authentification

On doit partir du principe que pour les cas où une identification officielle est nécessaire, l'authentification doit aussi être forte. Dès lors, il est recommandé d'évaluer les processus liés à l'enregistrement, l'identification ou l'authentification dans une analyse de risques et une définition de mesures commune.

6 Vue d'ensemble des cas d'application

En principe, on peut classer les services en cinq cas d'application distincts. Les exigences liées à l'identification et à l'authentification ainsi que les mesures à prendre doivent être analysées pour chaque cas individuel.

Pour chaque cas on peut distinguer s'il peut être géré sans ou avec authentification. La combinaison de données personnelles – par exemple le numéro d'immatriculation d'un véhicule et le nom – peut aussi être considérée comme authentification.

Cas d'application	sans authentification	avec authentification
1. cas de „l'information unique" Communication ou accès unique à des informations sous forme anonyme	• Publication de News et manifestations sur un site internet • Accès à des informations sous forme simple et anonyme auprès d'un organe public • Accès à des informations sous forme anonyme, comme des News communales, le calendrier d'élimination des déchets (anonyme), des manifestations, les vacances scolaires • Téléchargement de formulaires, documents, normes, circulaires, brochures etc. • …	• n/a

Cas d'application	sans authentification	avec authentification
2. cas de „l'information répétitive" Accès ou réception répétitive d'une information sous forme anonyme	• abonnement à des informations, p.ex. un Newsletter par E-Mail • …	• n/a
3. Cas de „l'information personnalisée" Communication personnalisée par l'autorité	• n/a	• commande fréquente • news communales et manifestations sous forme personnalisée • abonnement à des informations personnalisées et de manifestations, sous communication des intérêts, du lieu etc. comme des news communales, un calendrier d'élimination des déchets, manifestations, vacances scolaires • horaire d'école présenté de manière individuelle, par élève • Téléchargement de formulaires remplis • …
4. Cas d'application „opération simple avec l'autorité" Opérations simples et communication avec des autorités, p.ex. des questions, commandes, annonces etc.	• Annonce concernant l'état d'une infrastructure communale (un réverbère ne fonctionne pas) • Question soumise à un organe (question liée à la protection des données posée au préposé) • Commande d'une chronique communale • Commande d'une carte de parking • Commande d'une carte journalière CFF • Inscription pour le contrôle du véhicule auprès de l'office de la circulation routière • …	• Commande d'une carte de parking avec reprise des données de l'ancienne commande/choix du véhicule utilisé par le requérant • L'inscription pour le contrôle du véhicule auprès de l'office de la circulation routière avec reprise des données de l'ancien contrôle/choix du véhicule utilisé par le requérant • Commande d'une carte journalière CFF avec reprise des données de mon adresse • E-déménagement: communication d'un changement de domicile • …
5. Cas de „l'opération complexe avec l'autorité" Echange de données dans le cadre d'une procédure avec interaction et collaboration de l'autorité	• n/a	• Interaction répétitive avec l'habitante/l'habitant et l'autorité: • Procédure d'autorisation (p.ex. autorisation de travail) • Dépôt et gestion de demandes d'autorisation de construire

Cas d'application	sans authentification	avec authentification
		• Dépôt de la déclaration d'impôts • Demande d'aide sociale, bourse d'étude • …

Tableau 4: Vue d'ensemble des cas d'application avec/sans authentification

7 Les aspects juridiques

Beaucoup de facteurs influencent la réponse à la question de savoir, si et à quel niveau il convient d'édicter une base légale pour l'exploitation d'un portail web par un organe public. Les conditions prévues par la loi cantonale sur la protection des données peuvent être l'un de ces facteurs. Dans chaque cas individuel, il convient d'analyser la situation sur un plan factuel et juridique.

A cet effet, il convient en particulier de répondre aux questions suivantes:
- De quel type de portail s'agit-il? Quelles applications spécialisées peuvent être reliées au portail? De combien d'applications spécialisées parlons-nous?
- Est-ce que des données personnelles sont sauvegardées par le portail, jusqu'à ce qu'elles soient exportées dans l'application spécialisée?
- Quelles données (personnelles sensibles ou non) sont traitées par quels organes et à quelle finalité?
- Combien de données personnelles sont sauvegardées dans le portail (y a-t-il constitution d'un profil de la personnalité en fonction d'un nombre élevé d'opérations)?
- Sur la base de quelles bases légales, l'organe public traite-t-il des données de l'application spécialisée?

Sur la base des réponses apportées aux questions précédentes, respectivement sur la base des circonstances du cas individuel, on pourra déduire le contenu, la précision nécessaires et le niveau législatif d'une éventuelle base légale. La base légale édictée doit tenir compte de l'aménagement concret du portail.

Si un organe exploite tout seul un portail qui ne contient que des données de cet organe, aucune base légale n'est nécessaire dans la mesure où le traitement de données est lié à une tâche clairement décrite par la loi. Dès que le portail web comporte les données de plusieurs organes ou que plusieurs organes peuvent y accéder voire qu'une authentification forte est nécessaire, une base légale devient nécessaire. Celle-ci doit en particulier régler les responsabilités.

Si on veut organiser un échange de données entre organes par le biais d'un portail non couvert par une base légale existante, il faut édicter une nouvelle base légale.

En fonction d'une future extension d'un portail, il sera possible de procéder par étapes pour la création d'une base légale, en admettant d'abord une réglementation interne, puis une ordonnance et, enfin, une loi formelle. Si, toutefois, cette extension du portail est planifiée dès le départ, il est conseillé de prévoir tout de suite une loi au sens formel.

Sur le plan de la protection des données, d'autres sujets doivent être abordés en relation avec les portails web:

- Identificateur et son usage (interne à l'administration)
- Données personnelles traitées par le portail: la base légale doit indiquer quelles données personnelles sont traitées par le portail web.
- Compétences
- Responsabilités organisationnelles et financières
- Droits d'accès
- L'échange d'information entre organes publics au travers du portail
- Sauvegarde (passagère) de données personnelles dans le portail
- Effacement des données et des comptes (cas [p.ex. décès], modalités)

Selon l'aménagement concret du portail, ces sujets doivent être réglés dans une loi formelle. De toute manière, il est pertinent et conseillé sur le plan de la protection des données de prévoir une réglementation obligatoire et interne à l'organe, afin de traiter les sujets les plus importants liés au portail en question.

Le lien suivant permet de voir un exemple de loi concernant les portails web des autorités publiques: http://www.gesetzessammlung.bs.ch/frontend/versions/4076.

8 Mesures organisationnelles et techniques

Afin de pouvoir garantir la sécurité des données d'un portail web, de nombreuses exigences organisationnelles et techniques doivent être respectées. Les objectifs de protection (confidentialité, disponibilité, traçabilité et intégrité) doivent être réalisés à l'aide de mesures adéquates. Les mesures doivent être définies à l'aide d'une analyse des risques à intervalle régulier, prenant en compte l'état technologique et les standards reconnus. La responsabilité pour l'analyse et l'évaluation des risques et la définition de mesures de protection doivent être définies de manière claire, dans le cadre d'une responsabilité technique globale. Les principes de Privacy by Design et Privacy by Default doivent être mis en œuvre de manière conséquente.

Lors de la création et de l'exploitation du portail, il convient notamment de prendre en compte les points suivants:

- Les processus et actions pour l'administration des utilisateurs et l'authentification doivent répondre aux exigences de l'opération choisie et doivent être réalisés.
- La transmission de données (data in transport) et leur sauvegarde (data at rest) doivent être soumis aux mesures cryptographiques adéquates, en particulier s'il s'agit de données personnelles sensibles.
- Pour le développement, il convient d'appliquer un processus qui favorise la sécurité des données.
- Il convient de prendre des mesures pour la migration du Top-10 des failles de sécurité[1] selon l'Open Web Application Security Projects (OWASP).
- Les utilisatrices et utilisateurs doivent être informés sur les risques liés à l'utilisation du portail.
- Les droits d'accès doivent être documentés et vérifiés de manière périodique.
- Des événements qui mettent en jeu la sécurité doivent faire l'objet d'un protocole et

1 OWASP Top Ten Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

être analysés périodiquement.

9 Le nom de l'utilisatrice ou de l'utilisateur comme identificateur univoque

Par la mise en place d'un portail central, les utilisatrices et utilisateurs ne doivent s'inscrire plus qu'avec une seule identité, afin d'accéder à diverses applications spécialisées. Sur le plan de la protection des données, ce point comporte des risques, dans la mesure où cette identité est univoque pour chaque système et chaque utilisatrice et utilisateur. Le nom d'utilisatrice ou d'utilisateur peut donc être utilisé comme identificateur univoque pour les applications spécialisées (pour ce qui est de la discussion liée à l'utilisation du numéro AVS voir[2]). Sur un plan technique, on dispose de moyens qui permettent d'avoir un accès distinct pour chaque application spécialisée, notamment en fonction d'une reconnaissance individuelle et pseudonyme. Il convient de vérifier pour chaque cas individuel, en fonction des risques encourus, si un accès pseudonyme par application spécialisée est nécessaire ou si un accès général peut être considéré comme suffisant.

10 Délimitations

10.1 Délimitation par rapport à l'eVoting

Le sujet de l'eVoting (vote par voie électronique) n'est pas traité par le présent document, car il existe des exigences particulières liées à l'identification, l'authentification, l'autorisation, la protection des données, l'anonymat (secret de vote) et la sécurité des données, par rapport au portail ordinaire, mis à disposition pour des interactions avec les autorités. La réponse à des questions délicates liées au eVoting dépasse clairement le cadre du présent document. Pour plus d'informations, il est renvoyé aux articles spécialisés et aux débats comme l'«Essay Securing Elections»[3] de BRUCE SCHNEIER.

10.2 Délimitation par rapport à l'intermédiaire des données (Data Broker)

Dans le cadre de l'évolution de la digitalisation, la question de l'échange électronique de documents publics ou privés entre l'Etat (au niveau communal, cantonal ou fédéral), les privés et les utilisatrices et utilisateurs pour des opérations relevant du public ou du privé va certainement se poser toujours plus (p.ex. un extrait des données fiscales pour l'obtention d'un crédit hypothécaire ou des documents bancaires pour une déclaration d'impôts). Un tel échange est souvent réalisé par l'entremise d'un intermédiaire. Les exigences juridiques, organisationnelles et techniques liées à cette fonction sont tellement complexes, qu'elles dépasseraient le cadre du présent document. Il est proposé de traiter cette question dans un document séparé.

---

2 privatim, Verwendung der AHV-Nummer mit hohen Risiken verbunden, 16. Oktober 2017 (pas disponible en langue française), http://www.privatim.ch/de/verwendung-der-ahv-nummer-mit-hohen-risiken-verbunden/

3 BRUCE SCHNEIER, Securing Elections, 10. Mai 2017, https://www.schneier.com/blog/archives/2017/05/securing_electi.html

11 Vue d'ensemble des applications eGOV en Suisse

Le tableau ci-dessous comporte une vue d'ensemble des applications eGovernment actuelles et connues sur un plan cantonal. Il ne s'agit pas d'une énumération exhaustive.

Organe public	**Description**	**Identification/ Authentification**	**Cas d'application (1, 2, 3, 4, 5)**	**Statut**
Sites internet PPDD	Site internet avec informations, circulaires et formulaire de contact	• Anonyme	1	Online
Canton de Zoug (Zuglogin)	Accès online aux dossiers administratifs et aux données administratives	• Numéro d'identification univoque • mTAN • Suisse ID	3, 4, 5	Online, déclaration fiscale dès 2018
Ville de Zoug	ID-Citoyen sur la base d'une Blockchain	• Blockchain	Pas de détails connus actuellement	Online
Canton de Schaffouse	ID-Citoyen prévu avec l'entreprise Procivis, basé sur une application «eID+»	• Application qui sauvegarde l'ID	3, 4, 5	Online, depuis décembre 2017
Portail fiscal ZH	Portail web fiscal du canton de Zurich	• Enregistrement du code d'accès • Suisse ID • PW + mTAN	5	Online
edéménagement	edéménagement – le déménagement électronique	• Annonce d'un changement d'appartement	4	Online
efacture LU	Transmission électronique du et au canton de Lucerne	• Informations de la facture	4	Online
eBAGE+ LU	Demande d'autorisation de construire géré par voie électronique	• Formulaire électronique online	5	Online
Administration fiscale cantonale	Portail web fiscal du canton de Berne	• Enregistrement à l'aide d'un code d'accès et d'un Code-ID remis par courrier	5	Online
Canton de Berne	BE-Login: plateforme électronique du canton de Berne pour des services choisis	• Processus d'enregistrement avec adresse E-Mail, mot de passe, ID fac. ou passeport • Critère de sécurité mTAN ou carte code pour services avec niveau de sécurité 2	4, 5	Online

Organe public	**Description**	**Identification/ Authentification**	**Cas d'application (1, 2, 3, 4, 5)**	**Statut**
Prestations Abraxas (diverses communes ZH)	Diverses prestations online: • DF finances et débiteurs • DF e-facture • Gestion du recouvrement et des actes de défaut de biens • Nouveaux impôts • ZP ZüriPrimo • Loganto pour habitants • WEG eau, électricité et gaz	• Enregistrement au moyen du numéro AVS • Nom d'utilisatrice/ utilisateur et mot de passe • Suisse ID	3, 4, 5	Online

Tableau 5: Vue d'ensemble et classification des applications eGOV