

Protection des données

Dr. iur. Sandra Husi-Stämpfli, LL.M., Executive MPA

Dr. iur. Anne-Sophie Morand, LL.M., Avocate

Prof. iur. Ursula Sury, Avocate

Livio di Tria, MLaw, CIPP/E, CIPP/M

David Dias Matos, MLaw

Avec la relecture de Charlotte Beck

Table des matières

Avant-propos des éditeurs	V
Avant-propos des Autrices et Auteurs	VII
Sommaire	IX
Table des abréviations	XI
Bibliographie générale	XIX
Publications officielles	XXI
I. Chapitre: Introduction	1
A. Entrée en matière	2
B. Cas introductif	4
C. Pourquoi la protection des données est-elle (souvent) importante?	5
D. Évolution du droit suisse de la protection des données	7
1. La période entre 460 et 370 av. J.-C. : Hippocrate ouvre la voie	7
2. 20 ^e siècle : Le droit de la protection des données fait son entrée dans les systèmes juridiques	7
3. 21 ^e siècle : Protection des données et numérisation	8
a. 1 ^{re} impulsion : Révision de la protection des données dans l'UE	8
b. Révision suisse : Vers une loi moderne	9
c. Excursus : Les développements dynamiques au niveau de l'UE – un guide pour la Suisse	11
II. Chapitre: Cadre juridique	17
A. Entrée en matière	18
B. Cas introductif	19
C. Protection de la personnalité au regard de la Constitution et des droits fondamentaux	20
1. Aperçu	20
2. Art. 10 et 13 Cst.	22
a. Droit à la vie et liberté personnelle (art. 10 Cst.)	22

b. Droit à la protection de la sphère privée (art. 13 Cst.) ...	23
3. Sujets de la protection de la personnalité	24
D. Protection de la personnalité en droit civil	25
1. Aperçu	25
2. Protection de la personnalité contre les atteintes illicites de tiers (art. 28 CC)	26
a. Contenu et objectif de la protection	26
b. Atteinte à la personnalité	28
c. Motifs justificatifs d'une atteinte à la personnalité	28
aa. Consentement	28
bb. Intérêt prépondérant privé ou public	29
cc. Loi	30
d. Recours en matière de protection de la personnalité en droit civil, moyens défensifs et moyens réparateurs	30
E. Protection de la personnalité en vertu de la législation sur la protection des données	31
1. Répartition des compétences fédérales	31
2. Droit général et droit spécial de la protection des données	32
a. Droit général de la protection des données	32
b. Droit spécial de la protection des données	33
aa. Organes publics	33
bb. Personnes privées	34
III. Chapitre: But et champ d'application de la LPD	35
A. Entrée en matière	36
B. Cas introductif	37
C. Buts	38
D. Champ d'application à raison de la personne	38
E. Champ d'application à raison de la matière	39
1. Données relatives aux personnes physiques	39
2. Exceptions et délimitations	40
a. Exceptions au champ d'application de la LPD	40
b. Délimitations	40
aa. Droit procédural	40

(1) Notion de procédures judiciaires et procédurales fédérales	41
(2) Critère de rattachement	42
bb. Les registres publics relatifs aux rapports de droit privé	43
cc. Délimitation de la protection de la personnalité selon la LPD et le CP	44
F. Champ d'application territorial (Conflits de lois)	45
IV. Chapitre: Définitions	47
A. Entrée en matière	48
B. Cas introductif	49
C. Aperçu – Définitions de l'art. 5 LPD	51
D. Données personnelles (let. a)	52
1. Définition	52
2. Données anonymisées	53
3. Données pseudonymisées	54
E. Personne concernée (let. b)	55
F. Données personnelles sensibles (let. c)	55
1. Données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales (ch. 1)	56
2. Données relatives à la santé (ch. 2)	56
3. Données relatives à la sphère intime (ch. 2)	57
4. Données relatives à l'origine raciale ou ethnique (ch. 2) ...	57
5. Données génétiques (ch. 3)	57
6. Données biométriques (ch. 4)	58
7. Données sur des poursuites ou sanctions pénales et administratives (ch. 5)	58
8. Données sur des mesures d'aide sociale (ch. 6)	58
G. Traitement (let. d)	59
H. Communication (let. e)	61
I. Profilage (let. f)	62
1. Notion	62
2. Approche fondée sur les risques: profilage à risque élevé	63

J. Violation de la sécurité des données (let. h)	65
K. Organe fédéral (let. i)	66
1. Notion	66
2. La tâche publique de la Confédération comme critère de rattachement	66
L. Responsable du traitement (let. j)	69
M. Sous-traitant (let. k)	71
1. Définition	71
2. Délimitation par rapport au responsable du traitement ...	73
3. Tous les prestataires de services ne sont pas des sous-traitants	73
4. Contrat de sous-traitance	75
V. Chapitre: Principes généraux	79
A. Entrée en matière	80
B. Cas introductif	81
C. Généralités	82
D. Les principes généraux en détail	84
1. Principe de licéité	84
2. Principe de la bonne foi	86
3. Principe de proportionnalité	86
a. Traitement adéquat, nécessaire et proportionné	86
b. Mise en œuvre pratique	89
4. Principe de finalité	90
a. Collecte de données pour une finalité déterminée	90
b. Destruction et anonymisation lorsque la finalité n'est plus poursuivie	93
5. Principe de reconnaissabilité (ou transparence)	94
6. Principe d'exactitude	95
VI. Chapitre: Protection des données dès la conception et par défaut	99
A. Entrée en matière	100
B. Cas introductif	100

C. Contexte	101
D. Objectifs de la norme et aspects généraux	102
1. Champ d'application personnel	104
2. Champ d'application matériel	105
E. Protection des données dès la conception (<i>privacy by design</i>)	105
1. Objectif	105
2. Moyens: Technologies et organisations au service de la protection des données	106
a. Mesures techniques et organisationnelles	107
aa. Mesures techniques	107
bb. Mesures organisationnelles	108
b. Critères d'évaluation	108
F. Protection des données par défaut (<i>privacy by default</i>)	110
1. Objectif	110
2. Moyens: préreglages appropriés	110
VII. Chapitre: Sécurité des données	113
A. Entrée en matière	114
B. Cas introductif	115
C. Remarques préliminaires	115
D. Notion de sécurité des données	116
1. Pas de définition dans la loi	116
2. Nuance de la notion de sécurité des données dans l'OPDo	117
3. Standards internationaux et <i>best practices</i>	118
E. Champ d'application personnel de l'art. 8 LPD	119
F. Objectifs de protection	120
1. Confidentialité	120
2. Disponibilité	120
3. Intégrité	121
4. Traçabilité	121
G. Détermination des mesures techniques et organisationnelles appropriées	121
1. Méthodologie	121
2. Première étape: Évaluation du besoin de protection	123

a. Type de données traitées	123
b. Finalité, nature, étendue et circonstances du traitement	123
3. Deuxième étape: Évaluation du risque	124
a. Causes du risque	124
b. Principales menaces	124
c. Mesures prises ou prévues pour réduire les risques ...	125
d. Probabilité et conséquences d'une violation de la sécurité des données malgré les mesures prises	128
4. Troisième étape: Choix des mesures techniques et organisationnelles	128
5. Processus dynamique	129
VIII. Chapitre: Codes de conduite	131
A. Entrée en matière	132
B. Cas introductif	132
C. Codes de conduite	133
1. Objectif des codes de conduite	133
2. Destinataires de la norme (al. 1)	134
3. Contenu des codes de conduite	134
4. Caractère volontaire des codes de conduite	135
5. Prise de position du PFPDT sur les codes de conduite	135
IX. Chapitre: Certifications	137
A. Entrée en matière	138
B. Cas introductif	138
C. Certifications	139
1. Remarques préliminaires	139
2. Destinataires de la norme	139
3. Objet de la certification	140
4. Critères de certification	141
5. Qui certifie ?	141
6. Procédure et surveillance du PFPDT	142

X. Chapitre: Traitement par des personnes privées	143
A. Entrée en matière	144
B. Cas introductif	145
C. Responsabilité au sein de l'entreprise	146
D. Atteintes illicites à la personnalité causées par certains traitements de données	148
1. Atteintes à la personnalité	148
2. Motifs justificatifs	149
a. Consentement	150
b. Intérêt privé ou public prépondérant	152
c. Loi	154
E. Actions visant à protéger la personnalité	155
F. Traitement des données personnelles par des responsables du traitement privés ayant leur siège ou leur domicile à l'étranger	156
1. Représentant (art. 14 LPD)	156
2. Obligations du représentant (art. 15 LPD)	157
 XI. Chapitre: Traitement des données par les organes fédéraux	159
A. Entrée en matière	160
B. Cas introductif	161
C. Préliminairement: Plusieurs responsables du traitement des données mais une seule responsabilité	162
D. Bases légales	163
1. Ancrage du principe constitutionnel de légalité	163
2. Base légale pour le traitement de données personnelles « ordinaires »	164
3. Base légale pour le traitement de données personnelles sensibles	164
4. Exception: Compétence du Conseil fédéral	165
5. Exception: Traitement sans base légale matérielle ou formelle	166
E. Essais pilotes	167
1. Besoin d'une législation dans un État de droit pour les essais pilotes	167

2.	Conditions cumulatives pour un essai pilote	168
a.	Uniquement des essais pilotes avec des données personnelles sensibles?	168
b.	Densité normative de la loi au sens formel	169
c.	Mesures appropriées prises aux fins de réduire au minimum les atteintes aux droits fondamentaux de la personne concernée	169
d.	Caractère indispensable de l'essai pilote	170
3.	Modalités avant et pendant la phase de test	171
a.	Régler l'essai pilote dans une ordonnance	171
b.	Autorisation par le Conseil fédéral, implication du PFPDT	172
c.	Pas d'histoire sans fin: Évaluation et durée limitée de l'essai pilote	172
F.	Traitement à des fins ne se rapportant pas à des personnes ..	173
1.	Nécessité d'une législation	173
2.	Finalité «ne se rapportant pas à des personnes»	174
3.	Conditions du traitement	175
G.	Activités de droit privé exercées par des organes fédéraux ...	177
 XII. Chapitre: Communication de données		179
A.	Entrée en matière	180
B.	Cas introductif	181
C.	Communication de données en général	183
D.	Par les organes fédéraux	183
1.	Principe de légalité	183
2.	Les exceptions: Communication sans base légale	184
a.	Caractère indispensable pour l'accomplissement d'une tâche légale	185
b.	Consentement de la personne concernée	185
c.	Protection de la vie ou de l'intégrité corporelle	185
d.	Publication des données personnelles par la personne concernée	186
e.	Communication pour faire valoir les droits du destinataire	186

3. Communication de données personnelles	187
4. Communication au moyen de services d'information et de communication automatisés	187
5. Motifs de restriction	188
6. Droit d'opposition	189
7. Cas particulier de la « communication » selon le principe de transparence (LTrans)	189
E. Communication de données personnelles à l'étranger	191
1. Qu'est-ce qu'un transfert de données personnelles à l'étranger ?	191
2. Qu'est-ce qui n'est pas un transfert de données personnelles vers l'étranger ?	192
3. Principes (art. 16 LPD)	193
a. Pays offrant un niveau adéquat de protection des données	193
b. Pays n'offrant pas un niveau adéquat de protection des données	195
aa. Clauses contractuelles types (SCC) spécifiques	196
bb. Autres garanties	199
4. Exceptions (art. 17 LPD)	201
XIII. Chapitre: Sous-traitance (<i>Outsourcing</i>)	203
A. Entrée en matière	204
B. Cas introductif	205
C. Traitement par les sous-traitants	206
1. Externalisation des tâches	206
2. Rappel: sous-traitant, responsabilité et privilège de communication	206
3. Conditions relatives à la sous-traitance	208
a. Sous-traitance fondée sur un contrat ou une loi	208
b. Cura in eligendo, in instruendo et in custodiendo	208
c. Pas d'interdiction de sous-traitance	210
4. Sous-traitance ultérieure (en cascade)	211
5. Sous-traitance à l'étranger	211

XIV. Chapitre : Obligations du responsable du traitement	213
A. Entrée en matière	214
B. Cas introductif	215
C. Devoir d'informer (et ses exceptions)	217
1. Devoir d'informer lors de la collecte de données personnelles (art. 19 LPD)	217
a. Généralités	217
b. Objectif des devoirs d'informer	217
c. Contenu minimal	218
d. Moment de l'information	219
e. Exigences quant à la forme	220
f. Déclarations relatives à la protection des données	220
2. Exceptions au devoir d'informer et restrictions (art. 20 LPD)	222
3. Devoir d'informer en cas de décision individuelle automatisée (art. 21 LPD)	224
a. Quand y a-t-il une décision individuelle automatisée ?	224
b. Possibilité pour la personne concernée de faire valoir son point de vue	226
c. Examen par une personne physique	226
d. Exceptions	226
e. Décisions individuelles automatisées émanant d'organes fédéraux	226
D. Obligations en matière de gouvernance	227
1. Généralités	227
2. Registre des activités de traitement	228
a. Obligation de tenir un registre des activités de traitement	228
b. Contenu du registre des activités de traitement	228
c. Prescriptions de forme	230
d. Exceptions à l'obligation de tenir un registre des activités de traitement	230
e. Conséquences en cas d'absence d'un registre des activités de traitements	231

3.	Autres obligations en matière de documentation	232
a.	Obligation de journalisation	232
aa.	En amont : Sécurité des données ou <i>privacy by design</i> ?	232
bb.	Destinataire de la norme	232
cc.	Étendue de l'obligation de journalisation	233
dd.	Conservation et accessibilité des procès-verbaux de journalisation	233
b.	Règlement de traitement	234
aa.	Destinataire de la norme	234
bb.	Contenu et forme	234
c.	Politique interne de protection des données	235
4.	Analyse d'impact relative à la protection des données personnelles	235
a.	Méthodologie et contenu	237
b.	Forme et durée de conservation	237
c.	Exceptions	238
d.	Conséquences en cas de risque élevé résiduel	238
E.	Annnonce des violations de la sécurité des données	239
1.	Objectif de la norme	239
2.	Destinataire de la norme	239
3.	Définition de la violation de la sécurité des données	239
4.	Obligation d'annoncer	241
a.	Au PFPDT	241
b.	À la personne concernée	241
aa.	Principe	241
bb.	Restrictions à l'obligation d'annonce à la personne concernée	241
c.	Contenu de l'obligation d'annonce	242
d.	Documentation	243
e.	Excursus : Obligation d'annoncer versus Droit de ne pas s'auto-incriminer	243
F.	Perspectives d'avenir : Obligation de signaler les cyberattaques	243
1.	Secteurs concernés	244

2. Cyberattaques à signaler	246
3. Contenu du signalement	247
4. Délai pour signaler	247
5. Effets sur les normes de protection des données	247
XV. Chapitre: Droits des personnes concernées	249
A. Entrée en matière	250
B. Cas introductif	251
C. Droits des personnes concernées en général	252
D. Droit d'accès	253
1. Le droit d'accès en tant qu'instrument clé de l'autodétermination informationnelle	253
2. Compétence	253
3. Étendue du droit d'accès	254
4. Modalités, coûts et délais	255
a. Modalités	255
b. Coûts	256
c. Délais	256
5. Restrictions au droit d'accès	257
a. Restriction dans une loi au sens formel et en cas d'intérêts prépondérants	257
b. Restriction en cas de demande manifestement infondée	257
c. Motif de restriction spécifique pour les responsables du traitement privés	258
d. Motif de restriction spécifique pour les organes fédéraux	258
e. Conséquences en cas de non-respect du droit d'accès	259
f. Privilèges des médias	259
6. Excursus: Délimitation par rapport au droit de consulter le dossier	259
E. Droit à la remise ou à la transmission des données personnelles (droit à la portabilité)	260
1. Objectif	260
2. Conditions	261

3. Étendue du droit à la portabilité	261
4. Format électronique couramment utilisé	261
5. Coûts	262
6. Effacement après la transmission	263
7. Restrictions au droit à la portabilité des données	263
8. Conséquences en cas de non-respect du droit à la portabilité des données	263
F. Droit de rectification et de s'opposer vis-à-vis des personnes privées	264
G. Actions contre les organes fédéraux: abstention, suppression, constatation du caractère illicite	265
XVI. Chapitre: Organes	269
A. Entrée en matière	270
B. Cas introductif	270
C. Conseiller à la protection des données	271
1. Sens et objectif de cette fonction	271
2. Conseiller à la protection des données en entreprise (art. 10 LPD, art. 23 OPDo)	272
3. Conseiller à la protection des données au sein des organes fédéraux (art. 10 LPD, art. 25 ss OPDo)	274
D. Préposé fédéral à la protection des données et à la transparence	276
1. PFPDT – Fonction ou personne?	276
2. Organisation	276
a. Indépendance institutionnelle, fonctionnelle et financière	276
b. Conditions personnelles	277
c. Durée du mandat	278
3. Tâches et compétences	278
a. Activité de conseil et de sensibilisation	278
b. Consultation sur les actes législatifs et les mesures de la Confédération	279
c. Élaboration de recommandations sur les bonnes pratiques	279

d. Registre des activités de traitement	280
e. Tâches selon la LTrans	280
f. Enquêtes concernant des violations des prescriptions de protection des données	281
g. Assistance administrative	283
h. Coopération avec l'Office fédéral de la cybersécurité (art. 41 OPDo)	285
i. Traitement de données personnelles par le PFPDT	285
XVII. Chapitre: Sanctions	287
A. Entrée en matière	288
B. Cas introductif	289
C. Remarques préliminaires	290
1. Une occasion manquée	290
2. Points communs aux infractions pénales	290
3. Applicabilité des dispositions générales du CP	291
4. Compétence	291
D. Violation des obligations d'informer, de renseigner et de collaborer	292
E. Violation des devoirs de diligence	292
F. Violation du devoir de discrétion	294
G. Insoumission à une décision	295
XVIII. Chapitre: Mise en pratique	297
A. Entrée en matière	298
B. Transformation numérique, le phénomène actuel	301
1. De quoi s'agit-il?	301
2. Attention aux écueils	302
a. Les projets de numérisation ne sont pas seulement des projets du service informatique	302
b. La numérisation des processus: Pas de reprise telle quelle du monde analogique	304
c. Les projets de numérisation impliquent également des questions juridiques	305

C. Souveraineté numérique de l'État	305
1. Souveraineté numérique: de quoi s'agit-il?	305
2. Considérations à prendre en compte dans le quotidien de l'administration, notamment lors du passage au <i>cloud</i>	306
3. La souveraineté numérique de l'État, un modèle en voie de disparition?	307
D. Quand l'État veut aller dans le <i>cloud</i> : considérations juridiques	309
E. Système de gestion de la protection des données	312
1. De quoi s'agit-il?	312
2. Pourquoi un système de gestion de la protection des données?	313
3. Exigences en matière de contenu d'un système de gestion de la protection des données	314
4. Autres exigences	316
F. Collaboration en ligne – pas de problème?	317
1. De quoi s'agit-il?	317
2. Questions juridiques	317
3. Considérations fondées sur les risques lors du choix d'un outil de collaboration en ligne	319
G. Plateformes en ligne et réseaux sociaux	321
1. Actualité	321
2. Qu'est-ce qu'une plateforme en ligne?	321
3. Aspects juridiques de la protection des données	323
a. Prescriptions générales en matière de protection des données	323
b. La question de la responsabilité	323
aa. Problème de fond	323
bb. Responsabilités sur les plateformes d'évaluation ..	324
c. La question du Big Data	324
d. Le Social-Media-Paradox	325
H. Cookies	325
1. Défi: Pister les miettes sur interne	325
2. Conditions légales	327
a. En Suisse	327

b. En Europe	328
3. Conseils pour l'utilisation de cookies	329
I. Gouvernance de la blockchain et de la DLT	329
1. Client de la blockchain	330
a. Qu'est-ce qu'une blockchain?	330
b. Trois caractéristiques clés de la blockchain	330
c. Comment fonctionne une blockchain?	331
d. Formes d'organisation	331
2. Questions relatives à la protection des données	332
a. Consentement?	332
b. Nécessité de publicité?	332
c. Respect des droits des personnes concernées	332
d. La question de la responsabilité et du droit applicable	333
e. Gouvernance de la blockchain	333
3. Blockchain: Mission impossible de la protection des données?	334
J. Internet of Things (IoT)	335
1. De quoi s'agit-il?	335
2. Réglementation de l'IoT	338
3. Gouvernance de l'IoT	338
4. Défis en matière de protection des données	338
a. Principes généraux	338
b. Sécurité des données et de l'information	339
K. Métavers	340
1. Qu'est-ce que le Métavers?	340
a. Rapprochement	340
b. Tentative de définition	340
c. Comment accéder au métavers?	341
2. Types de plateformes métavers	341
3. Espace économique du métavers	343
4. Métavers: <i>Hype</i> ou révolution à plus long terme?	343
5. Aspects juridiques du métavers	344
a. Principes de base	344
b. Le droit applicable	344

c. Les responsabilités	345
d. Sécurité dans le métavers	345
e. Protection des données dans le métavers	345
L. Self-Sovereign Identity	346
1. De quoi s'agit-il?	346
2. Qu'est-ce qu'une Self-Sovereign Identity?	347
3. Comment fonctionne la Self-Sovereign Identity?	348
4. Aspects de protection des données	350
M. Immersive Reality, VR, AR et MR	351
1. De quoi s'agit-il?	351
2. Variantes de réalités virtuelles (VR, AR, MR)	352
3. Cas d'application	353
a. Généralités	353
b. Cas du « <i>Digital Twin</i> »	354
4. Questions juridiques	355
a. Généralités	355
b. Aspects de la protection des données	355
aa. Licéité du traitement des données?	356
bb. Lieu et durée de conservation, autorisations d'accès	357
cc. Sécurité des données	357
dd. Besoin d'agir en matière de protection des données?	357
Index	359
Table des matières	371