Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 18. Jahrgang, Heft 3, September 2018

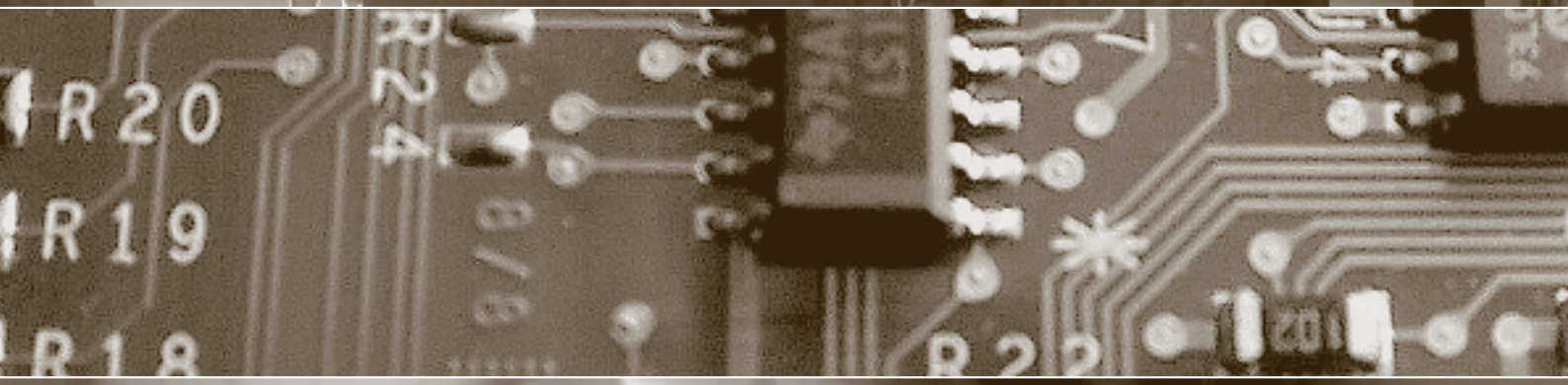
Schwerpunkt:

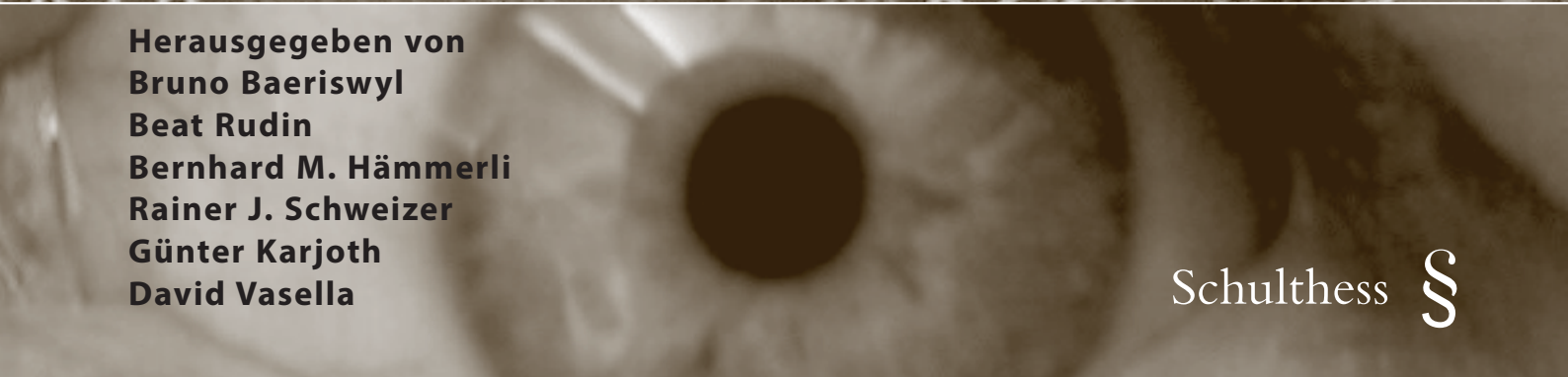
Cybersouveränität

fokus: Digitale Selbstbestimmung der Schweiz

fokus: Unterschätzte Risiken durch Lieferanten

report: RGPD en Suisse: mise en œuvre des sanctions





Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Cybersouveränität

auftakt
«Cyber» muss beim Bund ein Gesicht erhalten
von Joachim Eder Seite 81

Cybersouveränität: neun Sichtweisen
von Bernhard M. Hämmerli Seite 84

Digitale Selbstbestimmung der Schweiz
von Philipp Metzger/
Thomas Schneider Seite 86

EU Digital Autonomy: a possible apporach
von Luigi Rebuffi Seite 92

Cybersouveränität aus völkerrechtlicher Warte
von Anna Petrig/Maria Stemmler Seite 100

Disruption der Demokratie?
von Ursula Münch Seite 108

Sicherheitspolitik und digitale Souveränität
von Erich Vad Seite 114

Digitale Selbstbestimmung der Schweiz

Der Begriff «Cybersouveränität» ist international von Staaten besetzt, die das Internet auf nationaler Ebne kontrollieren wollen. Es sollte daher besser von «digitaler Selbstbestimmung» gesprochen werden. Wie setzt sich die Schweiz auf internationaler Ebene dafür ein?

Cybersouveränität aus völkerrechtlicher Warte

Wird durch Cyberoperationen die völkerrechtliche Souveränität eines Staates verletzt, hat dieser zwar ein Recht auf Selbstverteidigung und zur Ergreifung von Gegenmassnahmen. Aufgrund faktischer Hürden – namentlich fehlender eigener Cyberfähigkeiten zur Entdeckung und Zuordnung eines Angriffs und Ausführung eines digitalen Gegenschlags – greifen diese völkerrechtlichen Mittel der Selbsthilfe allerdings oft ins Leere. Politisch anzusetzen ist deshalb bei der Prävention gegen schädliche Cyberoperationen.

Sicherheitspolitik und digitale Souveränität

Angesichts der neuen Sicherheitsherausforderungen im Zuge der Digitalisierung braucht es dringend nachhaltige Konzepte und Strategien, um die öffentliche Sicherheit, die Sicherheitsvorsorge und vor allem Transparenz für die Bürgerinnen und Bürger und damit deren Vertrauen sicherzustellen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlu§: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlu§: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Tel. +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Unterschätzte Risiken durch Lieferanten

Mit der zunehmenden digitalen Vernetzung der Unternehmen im Cyber-Raum werden Anreize und Angriffsflächen für Attacken grösser. Unternehmen haben daher den Schutz ihrer eigenen Infrastruktur in den letzten Jahren stark verbessert. Doch wie kann sich ein Unternehmen gegen Angriffe auf seine Lieferanten schützen?

RGPD sur sol suisse: mise en œuvre

Die EU-Datenschutz-Grundverordnung kann auf Schweizer Unternehmen Anwendung finden. Wie werden allfällige von EU-Datenschutzbehörden ausgesprochene Sanktionen durchgesetzt werden?

Was klar scheint, muss nicht klar sein

Die EU-Datenschutz-Grundverordnung gilt auch, wenn Unternehmen in Drittstaaten Personen, die sich in der EU befinden, Dienstleistungen anbieten und in diesem Zusammenhang Personendaten über diese Personen bearbeiten. Alles klar?

Cybersouveränität

In einer zunehmend vernetzten Welt wird es auch zunehmend schwierig, die Souveränität sicherzustellen. Systemkomponenten müssen sorgfältig evaluiert werden. Unser Cartoonist war dabei …

fokus

Unterschätzte Risiken durch Lieferanten
von Dirk Fisseler/Jan Siegmund/
Nils Mörstedt/Tobias Krafft Seite 120

Digitale Souveränität – eine nationale Frage?
von Hartmut Jäschke/Peter Rost Seite 126

Cybersicherheit – Chance der Schweiz
von Marc Holitscher Seite 132

Konkurrenzfähig dank Cybersouveränität
von Adolf Dörig/Nicole Wettstein Seite 138

agenda Seite 137

report

Application du RGPD
RGPD sur sol suisse: mise en œuvre
von Yaniv Benhamou/
Emilie Jacot-Guillarmod Seite 142

Forschung
Einfache Zwei-Faktor-Authentisierung
von Marcel Waldvogel/
Thomas Zink Seite 150

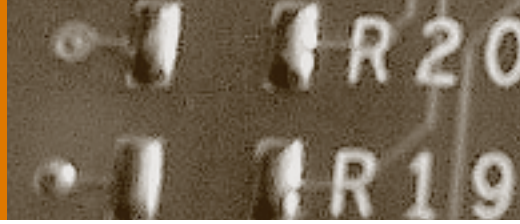
forum

privatim
Aus den Datenschutzbehörden
von Dominika Blonski Seite 154

Der Blick nach Europa und darüber hinaus
Was klar scheint, muss nicht klar sein
von Barbara Widmer Seite 158

schlusstakt
Blindflug der Berufsgeheimnisträger
von Beat Rudin Seite 160

cartoon
von Reto Fontana



Application du RGPD

RGPD sur sol suisse : mise en œuvre

Yaniv Benhamou, Lenz & Staehelin, Genève yaniv.benhamou@lenzstaehelin.com

Emilie Jacot-Guillarmod, Lenz & Staehelin, Genève emilie.jacot-guillarmod@lenzstaehelin.com

Les questions du champ d'application du RGPD (en particulier son champ d'application extra-territorial) et les obligations en découlant ont déjà fait couler beaucoup d'encre[1]. Les questions de mise en œuvre *(enforcement)*, en particulier la coopération avec les autorités européennes et l'exécution des sanctions européennes, ont été en revanche beaucoup moins thématisées[2].

Coopération avec les autorités européennes

Transmission directe par l'entreprise

La coopération avec les autorités européennes de contrôle risque de s'intensifier avec le RGPD. En plus des amendes administratives, dont l'exécution en Suisse est analysée ci-dessous, les autorités européennes de contrôle peuvent notamment mener des enquêtes (p.ex. demander tout type d'information et procéder à des audits). L'entreprise suisse aura tendance à coopérer, en particulier pour éviter des amendes administratives. L'entreprise suisse aura par ailleurs l'obligation de notifier à l'autorité les violations de données à caractère personnelle.

L'entreprise suisse pourra être ainsi amenée à coopérer directement avec les autorités de contrôle. Une telle coopération pose la question de savoir si l'entreprise commet un acte prohibé au sens de l'art. 271 CP. De prime abord, les conditions semblent remplies. La communication d'informations pour les besoins d'une procédure étrangère (civile, pénale ou administrative) constituerait un acte relevant « des pouvoirs publics », l'acte serait accompli « sans autorisation » en l'absence de procédure d'entraide ou d'autorisation délivrée par une autorité suisse et l'acte serait exécuté « sur le territoire suisse », même si les informations sont communiquées via le représentant UE ou le délégué à la protection des données (DPO) domicilié en UE, puisqu'il est suffisant que seule une partie des actes pertinents se réalisent sur sol suisse[3]. À y regarder de plus près, il faut distinguer différents scénarios.

L'acte exécuté par une entreprise suisse (en particulier la production de documents suite à une faille de sécurité ou à une demande de l'autorité européenne) ne devrait selon nous pas être un acte prohibé au sens de CP 271(1), tant qu'il concerne uniquement l'entreprise visée par la demande d'informations[4]. Selon plusieurs auteurs, CP 271(1) vise en effet à protéger la souveraineté suisse (en empêchant l'exécution, sur sol suisse, d'actes relevant des « pouvoirs publics », peu importe les caractéristiques de l'auteur de l'acte, fonctionnaire ou non, ou la qualification de l'acte à l'étranger),[5] mais pas à empêcher une personne localisée en Suisse *dans la défense de ses intérêts à l'étranger*[6].

Ce raisonnement basé sur la défense des intérêts de la personne visée par la mesure fait toutefois l'objet des tempéraments suivants :

- D'abord, ce raisonnement n'est pas partagé par l'OFJ, en tous les cas dans le domaine de l'entraide internationale en matière civile, pour qui le critère déterminant pour qualifier comme « acte relevant des pouvoirs publics » est que le refus de coopérer peut avoir des conséquences excédant la procédure civile, autrement dit la menace de sanctions pénales ou administrative *en cas de refus de coopérer*[7]. Ce raisonnement, transposé à la protection des données, conduirait à considérer que toute coopération avec les autorités européennes (la production de documents suite à une faille de sécurité ou à une demande de l'autorité européenne) tomberait sous le coup de CP 271(1). Ce raisonnement doit être toutefois rejeté

aux motifs qu'il n'a aucun fondement légal[8] et a été émis pour le domaine de l'entraide internationale en matière civile, et n'est ainsi pas nécessairement transposable à l'entraide en matière de protection des données.

- Ensuite, l'application d'éventuelles normes de confidentialité (p.ex. LB 47, LBVM 43, CP 162 ou 273) demeure réservée : la production d'informations doit naturellement s'effectuer dans le respect des éventuelles obligations de confidentialité[9]. L'entreprise suisse devra ainsi garantir la confidentialité, en particulier le secret bancaire, professionnel ou contractuel, notamment en communiquant uniquement les catégories de données personnelles ou des d*onnées personnelles anonymisées*[10].
- Enfin, la possibilité de produire librement des documents est limitée aux procédures étrangères auxquelles *la personne localisée en Suisse est partie* et dans le cadre desquelles cette dernière *défend ses propres intérêts*.

Vu l'incertitude créée par CP 271 lors de son application en matière de protection des données, en particulier vu les différentes définitions de l'acte relevant des pouvoirs publics, et l'évolution de la coopération internationale[11], il est souhaitable que la Suisse offre un cadre légal clair de la coopération internationale en matière de protection des données et que les autorités compétentes émettent une autorisation-cadre permettant la transmission d'informations ou négocient un accord d'entraide administrative.

Transmission par le Préposé suisse

Au regard du champ d'application extra-territorial du RGPD, certaines entreprises suisses seront soumises à la surveillance simultanée des autorités européennes et du Préposé suisse[12]. De ce fait, une coopération accrue entre le Préposé et les autorités européennes s'avèrera souhaitable. Les autorités européennes pourraient en outre souhaiter obtenir certaines informations directement du Préposé.

À titre liminaire, nous relevons qu'en pratique, la collaboration informelle entre autorités administratives suisses et européennes est fréquente dans de nombreux domaines. En particulier, l'échange entre autorités d'informations générales sur leurs activités ou leurs projets ne nécessite aucune base légale particulière[13]. En revanche, tout échange d'informations confidentielles relève de l'entraide formelle et requiert en principe une base légale, conformément au principe de la légalité. L'entraide peut se fonder sur une base légale de droit interne (fédéral ou cantonal), ou sur une convention internationale[14]. Le droit suisse ne connaît en l'état aucune base légale (interne ou conventionnelle) régissant généralement l'entraide administrative[15]. *De lege lata*, il n'existe pas non plus de convention internationale spéciale relative à l'entraide administrative dans le domaine de la protection des données[16].

La LPD actuelle contient des règles générales sur le transfert d'informations par les organes fédéraux (art. 19 ss LPD) et se limite pour le surplus à attribuer au Préposé la tâche de collaborer avec les autorités étrangères chargées de la protection des données (art. 31 al. 1 let. c LPD)[17]. Le Préposé peut ainsi collaborer avec les autorités étrangères et leur communiquer des informations, dans le respect des principes généraux de l'activité de l'État[18], en particulier le principe de la proportionnalité (art. 5 al. 2 Cst. féd.) qui interdit les requêtes exploratoires *(fishing expeditions)*[19], et de la protection des données. Aux termes de l'art. 19 al. 1 LPD, la communication de données personnelles par des organes fédéraux requiert en principe une base légale. Par exception, la LPD autorise les organes fédéraux à communiquer des données personnelles nonobstant l'absence de base légale dans certains cas, notamment (1) lorsque le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale (art. 19 al. 1 let. a LPD) ou (2) lorsque la personne concernée y a consenti en l'espèce (art. 19 al. 1 let. b LPD).

S'agissant du premier motif justificatif, il faut que l'absence de transmission des données empêche complète-

Résumé

Cet article analyse la mise en œuvre du RGPD en Suisse. Les auteurs constatent de nombreuses incertitudes quant aux interactions entre les cadres juridiques suisse et européen. Selon l'analyse présentée ici, les sanctions européennes ne sont pas directement exécutables en Suisse, mais peuvent donner lieu à des prétentions récursoires sur le plan civil. Selon les auteurs, les entreprises suisses peuvent sous certaines réserves coopérer avec les autorités européennes sans violer l'art. 271 CP.

ment l'autorité requérante de remplir sa tâche dans un cas concret[20]. Il convient à notre sens de se montrer exigeant dans l'appréciation du caractère nécessaire de la communication et de tenir compte des possibilités pour l'autorité requérante d'obtenir les informations directement de la personne concernée. Au regard des larges pouvoirs conférés aux autorités de contrôle européenne en vertu du RGPD, on peut s'attendre à ce que la transmission de données par le Préposé fédéral suisse soit rarement indispensable au sens de l'art. 19 al. 1 let. a LPD. Par opposition, il est probable que les entités suisses soumises à la fois à la LPD et au RGPD consentent à la transmission aux autorités européennes de certaines de leurs données en possession du Préposé fédéral suisse, afin d'éviter de devoir remettre plusieurs fois les mêmes informations aux différentes autorités compétentes.

Les règles générales relatives à la communication transfrontière de données (art. 6 LPD) s'appliquent en outre à l'échange d'informations avec des autorités étrangères. Ceci ne devrait pas poser de difficulté particulière, dans la mesure où la législation européenne assurant un niveau de protection adéquat à l'étranger.

La personne concernée a en principe le droit de s'opposer au transfert en faisant valoir un intérêt légitime (art. 20 LPD).

Précisons que la doctrine retient généralement que le principe de la spécialité (soit le fait que l'autorité requérante ne peut utiliser les informations transmises que dans le cadre de la procédure à la base de la demande d'assistance) s'applique en matière d'entraide administrative[22]. Partant, selon le droit en vigueur, il appartient au principe au Préposé de s'assurer que les autorités européennes n'utilisent pas les informations transmises à d'autres fins que celles de la protection des données[23].

Le P-LPD règle de façon détaillée l'assistance administrative entre le Préposé et les autorités étrangères chargées de la protection des données (art. 49 P-LPD). L'échange d'informations et de données personnelles entre le Préposé et une autorité étrangère chargée de la protection des données sera soumis notamment à l'exigence de la réciprocité et de la confidentialité (art. 49 al. 1 P-LPD)[24]. À notre sens, les autorités européennes rempliront en principe ces conditions, notamment au regard des dispositions pertinentes du RGPD (art. 50 RGPD)[25]. À notre sens, l'art. 49 P-LPD constitue une *lex specialis* par rapport aux dispositions générales sur la communication de données personnelles par les organes fédéraux (art. 32 s. P-LPD). En particulier, l'art. 49 al. 3 P-LPD prévoit l'information préalable de la personne concernée uniquement lorsque les données transmises sont susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires et dans la mesure où ceci ne nécessite pas d'efforts disproportionnés. Selon nous, cette disposition plus restrictive prime le droit général de la personne concernée de s'opposer à tout transfert de ses données personnelles (art. 33 P-LPD)[26], et permet la transmission de données sans information préalable lorsqu' aucun secret professionnel, de fabrication ou d'affaire n'est mis en péril. Cette évolution est contestable du point de vue du droit d'être entendu de la personne concernée[27].

Nous relevons que l'entraide sera accordée exclusivement pour l'accomplissement des tâches légales des autorités requérantes (art. 49 P-LPD). Par analogie avec l'entraide en matière financière, lorsqu'un acte pourrait tomber à la fois sous le coup du RGPD et sous le coup d'autres domaines juridiques (p.ex. violations de dispositions en matière pénale, fiscale voire du droit des obligations, des sociétés ou de la concurrence déloyale)[28], la matière faisant l'objet de l'assistance devrait être déterminée sur la base de la requête de l'autorité requérante[29]. En tout état, l'entraide en matière de protection des données ne devra pas permettre le contournement de l'entraide en matière fiscale[30] ou pénale[31]. Le P-LPD prévoit d'ailleurs expressément que l'autorité étrangère pourra utiliser les informations échangées uniquement dans le cadre de la procédure à la base de la demande d'assistance, conformément au principe de spécialité (art. 49 al. 1 let. b P-LPD).

Au regard de ce qui précède, le P-LPD permet plus largement la transmission d'informations par le Préposé suisse à ses homologues étrangers, notamment en l'absence de consentement des personnes concernées. Il a également le mérite de clarifier les modalités de l'entraide et l'utilisation possible des informations transmises. On peut en revanche regretter la limitation du droit d'être entendu de la personne concernée.

Exécution des sanctions

Généralités

Les autorités européennes de protection des données disposent a priori de divers moyens pour mettre en œuvre leurs décisions, en particulier

les sanctions prononcées, sur le territoire de l'UE. Elles privilégieront selon toute vraisemblance ces approches par rapport à une exécution dans un pays tiers. Cela étant, dans certaines circonstances, les autorités européennes devront rechercher l'exécution de leurs décisions en Suisse, par exemple parce que les actifs de la société concernée se trouvent en Suisse, parce que la société est dispensée de l'obligation de désigner un représentant en UE[32] ou a omis de le faire en violation de l'art. 27 RGPD. Selon le principe de la territorialité, la souveraineté suisse s'oppose généralement à l'exécution d'actes de puissance publique par des autorités étrangères sur le territoire helvétique[33]. Les autorités étrangères ne peuvent intervenir directement en Suisse[34], mais doivent requérir la reconnaissance et l'exécution par les instances suisses.

Par ailleurs, la mise en œuvre des décisions des autorités de surveillance européenne sur le territoire de l'UE peut donner lieu à des litiges subséquents entre le représentant européen et son mandant. En particulier, le représentant européen éventuellement tenu des sanctions prononcées à l'encontre de son mandant suisse peut chercher à se retourner contre ce dernier.

La présente section analyse les voies de droit ouvertes d'une part aux autorités européennes pour la mise en œuvre de leurs décisions en Suisse, et d'autre part au représentant européen pour agir à l'encontre du responsable suisse du traitement.

Qualification des décisions prises en vertu du RGPD

La procédure applicable en Suisse à l'exécution de décisions étrangères dépend du domaine du droit (administratif, civil, ou pénal) auquel ressortit la décision pertinente. La qualification s'opère selon le droit suisse[35].

A priori, les décisions prises par les autorités en application du RGPD (soit des mesures propres à influencer la situation juridique du destinataire prises par une autorité dans un cas concret[36]) constituent des décisions administratives au sens du droit suisse. En droit interne suisse, les sanctions prononcées par les autorités administratives ressortissent au demeurant au droit administratif[37].

Cela étant, la jurisprudence retient que les sanctions prononcées par les autorités administratives revêtent dans certaines circonstances une nature (matériellement) pénale[38]. Les critères de distinction entre le domaine pénal et le domaine administratif, et même la validité dogmatique de la notion de sanction administrative, sont d'ailleurs discutés en doctrine[39]. En l'absence d'une délimitation nette, exclure que les sanctions prononcées en vertu du RGPD puissent matériellement ressortir à la matière pénale nous paraît discutable. Une telle conclusion revêtirait en tout état peu d'intérêt pratique, dès lors que les règles en matière d'entraide pénale internationale posent des critères propres pour délimiter quelles décisions relèvent de leur champ d'application. L'éventuelle mise en œuvre des décisions prises en vertu du RGPD selon les règles applicables en matière d'entraide pénale internationale mérite ainsi l'examen.

Par ailleurs, si la protection des données relève en principe du droit public, elle peut donner lieu à des prétentions de droit privé[40]. Dans certains cas, la mise en œuvre transfrontière de la protection des données s'opère ainsi selon les règles de droit international privé[41]. En particulier, les différends entre le représentant européen et son mandant suisse relèvent du droit civil dans la mesure où ils opposent deux personnes privées. Partant, il sied d'examiner si les décisions prises en vertu du RGPD et/ou dans le cadre de litiges connexes peuvent (aussi) être mises en œuvre conformément au droit international privé suisse.

Entraide administrative

L'ordre juridique suisse ne connaît pas d'acte normatif régissant de manière générale la reconnaissance et l'exécution des décisions administratives étrangères. Il n'existe *de lege lata* aucune base légale particulière pour la reconnaissance et l'exécution en Suisse des décisions européennes en matière de protection des données. Ainsi, en l'état, le droit suisse ne permet pas la reconnaissance et l'exécution des décisions prises en vertu du RGPD par les autorités européennes au titre de l'entraide administrative.

Le P-LPD ne prévoit pas non plus de telle base légale. L'entraide administrative que pourra accorder le Préposé fédéral à teneur du P-LPD[42] n'équivaut aucunement à une mise en œuvre des décisions des autorités étrangères. En particulier, les compétences du Préposé fédéral en la matière ne permettent pas l'exécution de sanctions étrangères en Suisse. Si certaines démarches politiques ont été initiées en vue de la conclusion avec l'UE d'un accord relatif à la coordination en matière de protection des données, elles restent à un stade embryonnaire[43]. Au demeurant, nous relevons que si un accord de coopération a été conclu pour régler une situa-

tion internationale analogue en matière de droit de la concurrence[44], soit l'existence d'une double réglementation (les législations suisse et européenne étant susceptibles de s'appliquer au même état de fait) sanctionnée par des amendes très importantes prononcées par des autorités administratives, cet accord se limite à la coordination des procédures et à l'échange d'informations, à l'exclusion de la reconnaissance et l'exécution transfrontière des sanctions. On peut dès lors se demander si un futur accord bilatéral en matière de protection des données, s'il vient à chef, prévoira la reconnaissance et l'exécution des sanctions européennes en Suisse. En toute hypothèse, l'adoption dans un futur proche d'une base légale pour l'exécution des décisions en vertu du RGPD au titre de l'entraide administrative paraît peu vraisemblable.

Entraide pénale internationale

La Loi fédérale sur l'entraide en matière pénale (EIMP)[45] permet à certaines conditions l'exécution en Suisse de décisions étrangères en matière pénale. La qualification comme décision en matière pénale au sens de l'EIMP s'opère en principe selon les critères (matériels) de la jurisprudence *Engel*[46]: une sanction est pénale lorsque, alternativement, le droit national la classifie comme telle, ou lorsque la nature de l'infraction ou la gravité de la sanction en dénotent le caractère pénal[47]. Le droit européen qualifie les sanctions prononcées en vertu du RGPD d'amendes administratives[48]. Cela étant, au regard de la gravité des sanctions potentielles, qui peuvent atteindre 4% du chiffre d'affaires annuel mondial total de l'exercice précédant l'infraction, celles-ci revêtent à notre sens un caractère matériellement pénal au sens de la jurisprudence *Engel*[49].

L'entraide internationale en matière pénale n'est ouverte que pour les affaires dans lesquelles le droit de l'État requérant permet de faire appel au juge (critère formel) (art. 1 al. 3 EIMP). La pratique suisse est souple[50]. Les autorités suisses ont ainsi accordé l'entraide à des autorités administratives, dans la mesure où l'intervention de ces dernières constituait une étape préalable à la saisine des autorités judiciaires compétentes[51].

Nonobstant ce qui précède, en application de l'art. 1 al. 3 EIMP, le Tribunal fédéral exige que la répression des infractions à l'origine de la demande d'entraide relève de la compétence des autorités judiciaires de l'État requérant. Pour un éventuel octroi de l'entraide en matière pénale, il est ainsi nécessaire que la procédure puisse aboutir au renvoi d'accusés devant un tribunal compétent pour réprimer ces infractions[52]. Or, les autorités européennes en matière de protection prononcent elles-mêmes les sanctions prévues par le RGPD. L'intervention éventuelle d'une autorité judiciaire au stade du recours contre l'amende prononcée[53] ne satisfait à notre sens pas aux exigences de la jurisprudence fédérale susvisée. À défaut de possibilité de faire appel au juge au sens de l'art. 1 al. 3 EIMP, les sanctions prononcées en vertu du RGPD ne peuvent selon nous bénéficier de l'entraide pénale internationale.

Même si les autorités suisses devaient développer une approche plus souple et se satisfaire de la possibilité d'un recours devant une instance judiciaire, l'exécution en Suisse d'une décision pénale étrangère est notamment soumise à l'exigence de la double incrimination: l'état de fait sanctionné par l'autorité étrangère doit correspondre aux éléments constitutifs d'une infraction réprimée par le droit suisse[54]. Or, le champ d'application des sanctions du RGPD excède largement celui des sanctions pénales de la LPD actuelle et, dans une moindre mesure, du P-LPD.

Au regard de ce qui précède, même en admettant que les sanctions prononcées conformément au RGPD puissent bénéficier de l'entraide en matière pénale en Suisse[55], les autorités suisses refuseront vraisemblablement l'exécution des sanctions prononcées en vertu du RGPD dans un grand nombre de cas, à défaut de double incrimination.

En toute hypothèse, les autorités suisses n'exécutent la sanction prononcée à l'étranger qu'à concurrence de la peine maximale prévue par le droit suisse pour la même infraction[56], conformément au principe de la *lex mitior*[57]. Par conséquent, même si l'entraide en matière pénale internationale était octroyée en Suisse et si, dans le cas d'espèce, le droit suisse réprimait le comportement sanctionné par les autorités européennes, l'amende exécutée en Suisse ne saurait excéder 10000 CHF selon le droit actuel[58]. Sous réserve des débats parlementaires, ce maximum sera porté à 250000 CHF lors de l'entrée en vigueur du P-LPD[59]. Le risque encouru par les entités suisses recherchées directement sur le sol helvétique par les autorités européennes est ainsi en tout état largement inférieur aux peines maximales prévues par le RGPD (jusqu'à 20000000 EUR ou 4% du chiffre d'affaires mondial annuel).

Droit international privé

La Convention de Lugano (CL) régit la reconnaissance et l'*exequatur* en Suisse des décisions européennes ressortissant à la matière civile et commerciale, quelle que soit la nature de la juridiction (art. 1 al. 1 cum art. 62 CL). Il sied de relever que le domaine de la protection des données n'est pas exclu du champ d'application de la Convention (art. 1 al. 2 CL *a contrario*). En lien avec le RGPD, il faut à notre sens distinguer (1) la mise en œuvre des décisions prises par les autorités européennes de surveillance (notamment les amendes administratives), (2) celle des décisions prises en matière d'éventuelles prétentions récursoires du représentant européen contre son mandant suisse, et (3) des décisions prises en matière d'éventuelles prétentions récursoires de l'entité européenne à l'encontre de son coresponsable suisse.

S'agissant des décisions prises par les autorités européennes de surveillance, il est utile de rappeler que les décisions d'autorités administratives peuvent être reconnues et exécutées conformément à la Convention de Lugano, dans la mesure où elles ressortissent à la matière civile et commerciale[60]. Lorsque le rapport de droit implique une entité étatique, la Convention de Lugano s'applique si celle-ci agit de manière analogue à un privé. Par opposition, l'application de la Convention de Lugano est exclue lorsque l'autorité intervient en qualité de détentrice de la puissance publique[61]. Lorsqu'elles prononcent les mesures (en particulier les sanctions) prévues par le RGPD, les autorités européennes en matière de protection des données exercent

Notes de bas de page

1 P.ex. Préposé, Le RGPD et ses conséquences sur la Suisse, État : mars 2018; Fanti, Le nouveau Règlement général sur la protection des données et la Suisse : le nœud gordien de la double régulation et le fragile substrat législatif, in : Expert Focus 2017, 856. Plus spécifiquement sur le champ d'application territorial, cf. Daniel Ennöckl, ad article 3, 251, in : Gernot Sydow, Europäische Datenschutzgrundverordnung, Handkommentar, Baden-Baden 2017; David Vasella, Zum Anwendungsbereich der DSGVO, in : digma 2017, 221.

2 Voir toutefois la motion 16.3752 de Fiala Doris déposée le 28.9.2016 et acceptée par le Conseil fédéral le 9.11.2016 encourageant à des pourparlers entre le Conseil fédéral et les autorités européennes et à améliorer la coopération entre autorités suisses et européennes en vue d'une bonne application des législations respectives en matière de protection des données. Voir aussi Manuel Bergamelli, Die Auswirkung der neuen DSGVO auf die Schweiz, in : Jusletter 30 avril 2018.

3 CR CP II-Fischer/Richa, article 271 CP N 37 ; Précisons que CP 271 ne serait en revanche pas applicable, si toutes les informations sont localisées à l'étranger, p.ex. chez le représentant ou le DPO UE, faute d'une activité sur sol suisse.

4 CR CP II-Fischer/Richa, N 23. Cf. aussi les quatre décisions de 2016 relatives à des demandes d'autorisations adressées au DFJP et dans lesquelles le DFJP a rappelé la production de pièces dans une procédure civile étrangère par une partie n'est, en principe, pas un acte qui relève d'un pouvoir public suisse : JAAC 2016.3, 32-37 cons. 9; JAAC 2016.7, 56-61 cons. 9; JAAC 2016.8, 62-70 cons. 11.

5 ATF 114 IV 128, cons. 2a).

6 CR CP II-Fischer/Richa, article 271 CP N 22-32; BSK-Strafrecht II-Husmann, art. 271 N 32.

7 OFJ, Lignes directrices sur l'entraide judiciaire internationale en matière civile, 12. En faveur de cette approche : Boss Philippe Vladimir, 80, pour qui les quatre décisions citées à la n. 4 permettent de dégager une telle clé de définition.

8 CR CP II-Fischer/Richa, art. 271 CP N 27 : précisent que sinon toute personne répondant à une autorité au bénéfice d'un pouvoir de coercition exécuterait un « acte relevant des pouvoirs publics ».

9 CR CP II-Fischer/Richa, art. 271 N 23.

10 Modalité expressément prévue en cas de faille de sécurité (art. 33 al. 2 RGPD).

11 Qui a notamment conduit la Suisse à adopter des règles spéciales dans le domaine de la coopération internationale dans les domaines financiers (art. 42 ss LFINMA) et à l'adoption de nombreuses autorisations individuelles (cf. autorisation-modèle du 3 juillet 2013 en matière fiscale) et à un avant-projet de « loi sur la collaboration et la protection de la souveraineté » du 20 février 2013 destiné notamment à formaliser la pesée des intérêts à laquelle l'autorité suisse doit procéder avant de statuer sur l'octroi d'une autorisation au sens de CP 271 (abandonné par la suite aux motifs que les difficultés rencontrées dans la coopération avec les autorités étrangères peuvent être résolues sans passer par une loi).

12 Rapport de la Commission des institutions politiques du 12 janvier 2018 (<https://www.parlament.ch/centers/kb/Documents/2016/Rapport_de_la_commission_CIP-E_16.3752_2017-01-12.pdf>); Fanti, 859.

13 Pierre Moor/Alexandre Flückiger/Vincent Martenet, Droit administratif – Volume I : Les fondements, 3e éd., Berne 2012, 169.

14 Id., 170.

15 Précisons que la communication d'informations à des autorités européennes peut également reposer sur l'entraide internationale en matière pénale, notamment sur certaines conventions internationales liant la Suisse et l'UE, p.ex. la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 et la Convention sur la cybercriminalité du 23 novembre 2001. L'analyse des dispositions correspondantes dépasse le cadre de la présente contribution.

16 Contrairement aux standards internationaux (p.ex. IOSCO MMoU49 , IAIS MMoU50) ou accords bilatéraux entre la FINMA et les autorités étrangères en matière boursière et financière ou aux standards internationaux (p.ex. Convention modèle de l'OCDE ou Modèle d'accord sur l'échange de renseignement du Forum Mondial) et accords bilatéraux dans le domaine de l'entraide fiscale. Cela pourrait changer avec le P-LPD qui confère au Conseil fédéral la compétence de conclure des traités internationaux en matière de coopération internationale (art. 61 P-LPD). Précisons que dans certains cas, l'échange d'informations peut également reposer sur une convention internationale en matière pénale, par exemple la Convention sur la cybercriminalité du 23 novembre 2001.

17 Message P-LPD, 6710.

des pouvoirs réglementaires, de décision et de sanction[62]. Elles n'interviennent pas de façon analogue à un privé, mais exercent au contraire des prérogatives de puissance publique. Dans ces circonstances, leurs décisions ne ressortissent pas à la matière civile et commerciale au sens de la Convention de Lugano. Partant, la reconnaissance et l'exécution conformément à la Convention de Lugano est exclue. Par souci d'exhaustivité, on soulignera que les décisions prises en vertu de la puissance publique échappent également au champ d'application de la LDIP.

Les décisions prises dans le cadre de litiges opposant le représentant européen et son mandant suisse relèveront en principe du domaine contractuel. La matière contractuelle appartient au champ d'application matériel de la Convention de Lugano (art. 5 al. 1 CL). Le représentant européen et l'entreprise suisse peuvent élire un for en Suisse (art. 23 CL). Dans ce cas, le représentant fera valoir ses éventuelles prétentions récursoires directement devant les tribunaux suisses et la question de la reconnaissance ne se pose pas. En cas d'élection de for dans un État membre de l'UE, les décisions rendues par les tribunaux élus (art. 23 CL) sont reconnues (art. 33 ss CL) et peuvent être exécutées (art. 38 ss CL) en Suisse conformément à la Convention de Lugano. Si les parties ont omis d'élire un for contractuel, leur convention sera selon toute vraisemblance qualifiée de contrat de service au sens

Notes de bas de page (cont.)

18 Moor/Flückiger/Martenet, 968 ss.
19 ATF 129 II 484.
20 TAF, arrêt A-6320/2014 du 23 août 2016 cons. 8.1.
21 ATF 136 II 23; Moor/Flückiger/Martenet, 995.
22 Moor/Flückiger/Martenet, 992 s.; Amy, Entraide administrative internationale en matière bancaire, boursière et financière, 407.
23 Par analogie à la matière boursière et financière, cf. Amy, 407.
24 Ces principes se retrouvent dans d'autres domaines d'entraide, notamment l'entraide en matière boursière et financière (art. 42 al. 2 let. a et b LFINMA), qui prévoit toutefois davantage de règles spécifiques, en particulier lorsqu'il s'agit d'informations relatives aux clients (« procédure-client ») : la PA et les garanties procédurales en découlant sont applicables (art. 42a al. 2 LFINMA) mais il existe des assouplissements, soit une transmission sans notification au client ni procédure administrative préalables si une information préalable risquerait de compromettre le but de l'assistance administrative (en particulier en cas d'urgence particulière, p.ex. risque de collusion ou d'altération des preuves) (art. 42a al. 4 LFINMA). Homsy 13, n. 69.
25 Cf. également par. 61 Préambule RGPD.
26 Cette disposition correspond en substance à l'actuel art. 20 LPD, Message P-LPD, FF 6698 s.
27 Par analogie à la matière bancaire et financière, cf. Opel, Amtshilfe ohne Information der Betroffenen – eine rechtsstaatlich bedenkliche Neuerung, in : ASA 83 265 ss.
28 Homsy, n. 40.
29 FF 2004 6341, 6358 en matière boursière et financière : la matière faisant l'objet de l'assistance (les informations « nécessaires à l'exécution des lois sur les marchés financiers ») sera déterminée sur la base de la requête de l'autorité requérante.
30 Homsy, 8-9.
31 Message P-LPD, 6710.
32 À teneur de l'art. 27 al. 2 RGPD, les entités étrangères qui traitent les données de résidents européens de façon occasionnelle sont exemptées de l'obligation de désigner un représentant, à condition qu'elles ne traitent pas à large échelle certaines catégories de données sensibles.
33 Moor/Flückiger/Martenet, 156.
34 Cf. ci-dessus s'agissant des sanctions pénales encourues en cas de coopération à des actes de puissance publique d'autorités étrangères sur le territoire suisse.
35 En tant que tel, le fait que la lettre du RGPD mentionne des « amendes administratives » n'est ainsi pas déterminant.
36 Cf. art. 5 PA. Voir également Zufferey, La décision administrative – Un alibi au service de tous les intérêts, in : Mélanges Pierre Moor – Théorie du droit – Droit administratif – Organisation du territoire, 637 ss, 639.
37 Art. 1 DPA.
38 CourEDH, *Engel et autres cons. Pays-Bas*, N° 5100/51 du 8 juin 1976.
39 Pour une discussion détaillée, cf. p.ex. Niggli/Riedo, Quasi-Strafrecht, Strafrecht im engeren und weiteren Sinne und « Sozialethisches Unwerturteil », in : Amstutz et al. (éds), Die Praxis des Kartellgesetzes im Spannungsfeld von Recht und Ökonomie.
40 Arrêt du Tribunal administratif fédéral A-7040/2009 du 30 mars 2011 cons. 5.1 ss *(Google Street View),* Thalmann, Zur Anwendung des schweizerischen Datenschutzgesetzes auf internationale Sachverhalte, in : sic ! 2007, 337 ss, 338. À noter qu'en tant que telle, l'intervention des autorités administratives compétentes ne fait pas obstacle à l'application des règles de droit international privé. La doctrine postule ainsi que dans certains cas, le Préposé fédéral peut choisir le droit applicable aux atteintes à la personnalité résultant du traitement de données personnelles conformément à l'art. 139 LDIP, de manière analogue au lésé (Handkommentar DSG-Rosenthal/Jöhri, art. 29 LDP N 7 ; question laissée ouverte in Arrêt du Tribunal administratif fédéral A-7040/2009 du 30 mars 2011 cons. 5.5.2 *[Google Street View]).*
41 Arrêt du Tribunal administratif fédéral A-7040/2009 du 30 mars 2011 cons. 5.1 ss *(Google Street View),* Thalmann, 338.
42 Cf. ci-dessus.
43 Motion parlementaire intitulée « Pour éviter des doublons en matière de protection des données », adoptée par le Conseil national le 16 décembre 2016 et par le Conseil des États le 17 février 2017 (<https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163752%20Page>).
44 Accord entre la Confédération suisse et l'Union européenne concernant la coopération en matière d'application de leurs droits de la concurrence du 17 mai 2013.
45 Précisons que la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 ne prévoit pas la reconnaissance de décisions pénales étrangères.
46 BSK-Internationales Strafrecht-Fiolka, art. 1 EIMP N 36.
47 CourEDH, *Engel et autres cons. Pays-Bas*, N° 5100/51 du 8 juin 1976.
48 Art. 83 s. RGPD.

de la Convention. En cas de litige en lien avec un contrat de service, à défaut de convention contraire, la Convention de Lugano prévoit la compétence des tribunaux du lieu de fourniture du service (art. 5 al. 1 let. b CL). On peut dès lors s'attendre à ce que les tribunaux du lieu où le représentant européen déploie son activité soient compétents par défaut. Les décisions rendues par les tribunaux de l'État européen correspondant font l'objet d'une reconnaissance automatique (art. 33 CL) et peuvent donner lieu à l'*exequatur* (art. 38 ss CL) en Suisse.

Une éventuelle responsabilité partagée naîtra en principe entre des entités liées contractuellement (p.ex. contrat entre responsable du traitement et sous-traitant ou accord concernant la responsabilité conjointe du traitement). On peut dès lors renvoyer aux considérations qui précèdent en présence d'une clause d'élection de for et/ou lorsque les coresponsables sont liés par un contrat de service (notamment le contrat entre responsable du traitement et sous-traitant). Si la relation contractuelle entre coresponsables, en particulier entre *joint controllers*, ne peut être qualifiée de contrat de service au sens de la Convention de Lugano, le tribunal du lieu d'exécution de l'obligation litigieuse est compétent par défaut (art. 5 al. 1 CP). D'éventuelles prétentions récursoires se fonderont en principe sur les obligations incombant à la partie recherchée, soit l'entité suisse. On peut prévoir que le lieu d'exécution de ces obligations se situera régulièrement en Suisse, auquel cas le litige se déroulera directement devant les tribunaux suisses et la question de la reconnaissance ne se posera pas.

Conclusion

L'application extra-territoriale du RGPD a largement retenu l'attention des autorités et des auteurs suisses. La mise en œuvre transfrontière du droit européen s'avèrera cependant complexe.

En particulier, les sanctions prévues par le RGPD ne sont selon notre analyse pas directement exécutables en Suisse à ce jour. Cela étant, on ne peut exclure une mise en œuvre indirecte de ces sanctions, par le biais de la mise en œuvre à l'encontre d'une entité ayant une présence en UE (soit le représentant européen ou l'entité coresponsable du traitement, par exemple en qualité de *joint controller*) qui se retournerait ensuite sur le plan civil contre l'entreprise suisse.

Par ailleurs, des sujets peu thématisés jusqu'ici méritent à notre sens l'attention, notamment la possibilité pour les entreprises suisses de coopérer avec les autorités de surveillance européennes au regard de l'interdiction d'agir pour un État étranger sur le sol suisse (art. 271 CP). À ce sujet, nous recommandons une approche souple, qui permette à l'entreprise suisse de défendre ses propres intérêts à l'étranger, dans le respect d'éventuels devoirs de confidentialité.

De façon générale, nous constatons un manque de clarté quant aux futures interactions entre autorités suisses et européennes et aux implications pour les entreprises suisses soumises à une double réglementation. Dans l'intérêt de la sécurité juridique, une rapide clarification par nos autorités serait bienvenue. ■

Notes de bas de page (cont.)

49 Cette analyse est conforme à la jurisprudence en matière de droit de la concurrence, qui prévoit des sanctions similaires, Cf. ATF 139 I 72 ; CourEDH, arrêt Menarini Diagnostics S.R.L. cons. Italie du 27 septembre 2011, no 43509/08.

50 Cf. Art. 11 EIMP, à teneur duquel est « poursuivi » au sens de la loi tout suspect et toute personne contre lesquels une action pénale est ouverte ou une sanction pénale prononcée ; TF 1A.326/2005 du 1er mars 2006 cons. 2.2 ; BSK-Internationales Strafrecht-Fiolka, art. 1 EIMP N 36 ; CR EIMP-Moreillon art. 1 N 67.

51 ATF 113 Ib 257 ; 109 Ib 47 ; Arrêt du Tribunal fédéral 1A.326/2005 du 1er mars 2006 cons. 2.2.

52 Arrêt du Tribunal fédéral 1A.326/2005 du 1er mars 2006 cons. 2.2.

53 Les États-membres de l'UE doivent mettre en place un contrôle juridictionnel effectif contre les décisions prises par les autorités de contrôle en matière de sanctions (art. 83 al. 8 RGPD).

54 Art. 94 al. 1 let. b EIMP.

55 À notre sens, tel n'est pas le cas selon la jurisprudence actuelle, cf. ci-dessus.

56 Art. 94 al. 3 EIMP.

57 BSK-Internationales Strafrecht-Youssef/Heimgartner, art. 94 EIMP N 22.

58 Art 34 s. LPD *cum* art. 106 CP.

59 Art. 54 ss P-LPD.

60 BSK-LugÜ-Lerch/Rohner, Art. 1 CL N 37.

61 CJUE, arrêt C-29-76 du 14 octobre 1976, *LTU Lufttransportunternehmen GmbH & Co. KG cons. Eurocontrol* ; ATF 124 III 436 cons. 3.

62 Sur la notion de puissance publique, cf. Voisard, L'auxiliaire dans la surveillance administrative – Du droit bancaire et financier au droit administratif général, in : AISUF – Travaux de la Faculté de Droit de l'Université de Fribourg vol./no 333, 75 ss, N 160 ss.

Die wegweisende Fachzeitschrift zum Datenschutz

digma – die Zeitschrift für Datenrecht und Informationssicherheit greift quartalsweise umfassend und praxisorientiert interdisziplinäre Lösungsansätze aus Wirtschaft, Wissenschaft und Rechtsprechung auf und begleitet die Gesetzgebung und Diskussion rund um die Themen Datenschutz und Informationssicherheit.

- **Praxisrelevanz**

  Für die Praxis liefert digma fachlich fundierte Beiträge zu Datenrecht und zur Informationssicherheit.

- **Lösungsorientiert**

  digma sensibilisiert für aktuelle Probleme und zeigt interdisziplinäre Lösungsansätze aus Wirtschaft, Wissenschaft und Rechtsprechung auf.

- **Aktuell**

  Um auf dem Laufenden zu bleiben, informiert digma über neueste Entwicklungen und Trends.

- **Expertenwissen**

  Renommierte Experten berichten fundiert, kritisch sowie zukunfts- und lösungsorientiert über Datenrecht und Informationssicherheit.

digma

www.schulthess.com

Schulthess §

Schulthess §

Herausgeber:
Dr. iur. Bruno Baeriswyl,
Prof. Dr. iur. Beat Rudin,
Prof. Dr. Bernhard M. Hämmerli,
Prof. (em.) Dr. iur. Rainer J. Schweizer,
Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion:
Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin

Sprache: deutsch

☑ **JA,** ich profitiere vom **Mini-Abo** von **digma** und erhalte **2 Ausgaben** zum Kennenlernpreis von nur **CHF 58.–** (inkl. MWST und Versandkosten).

Vorname/Name

Firma

Strasse/Nr.

PLZ/Ort

E-Mail

Datum/Unterschrift

Abonnement-Bedingungen

Wenn ich digma danach weiterlesen möchte, muss ich nichts weiter tun und erhalte im Jahresabonnement 4 Printausgaben zum Preis von CHF 174.00 (inkl. MWST, zzgl. CHF 6.00 Versandkosten). Falls ich digma nicht weiter beziehen möchte, melde ich mich spätestens 7 Tage nach Erhalt der 2. Testausgabe bei Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich, E-Mail: service@schulthess.com, Fax: +41 (0)44 200 29 28.

A

Nicht frankieren
Ne pas affranchir
Non affrancare

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

Schulthess Juristische Medien AG
Kundenservice
Zwingliplatz 2
Postfach 2218
8021 Zürich