ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

DECEMBER 20, 2017

Data Protection Litigation to Become a New Reality in Belgium

By Jan Dhont, Lauren Cuyvers, and Dan Felz

On November 16, 2017, the Belgian Senate adopted an "Act on the Establishment of the Data Protection Authority." Following Austria, Germany, and the UK, Belgium is the fourth EU member state to pass a domestic statute implementing the General Data Protection Regulation 2016/679 (GDPR) before its effective date of May 25, 2018. The new Belgian Act sets forth the structure and legal organization of the data protection authority (DPA), which will supplant and serve as the successor to the current Belgian Privacy Commission. More importantly, the Act significantly broadens the DPA's powers. The DPA's function will evolve from being predominantly advisory to truly corrective, and even potentially punitive.

National Implementing Legislation Targeting DPA Powers

The Act was drafted in light of the GDPR, which entered into force on May 25, 2016, and will be enforceable in all EEA member states, including in Liechtenstein, Norway, and Iceland, starting May 25, 2018. As of that date, the current legislative data protection frameworks in the member states will no longer apply but will be replaced by the framework of the GDPR on the one hand and local legislation of the member states implementing the GDPR on the other. The GDPR requires and permits member states to adopt deviating or supplementing local laws in a number of areas, including the establishment of their local supervisory authority.

The Belgian Parliament took this opportunity to not only lay down the structure and organization of the new DPA, but also – for the first time – to clearly establish its competencies and its relation to other comparable supervisory agencies. In short, the Act expands the Privacy Commission's members to include at least six independent support agencies (supplemented further by independent experts and a "reflection council"), the most remarkable being an "inspection body" and a "dispute resolution chamber." These two agencies will each exercise true investigatory and corrective powers, comparable to powers exercised by a public prosecutor in criminal investigations. The most significant corrective powers exist in the imposition of administrative fines (up to the GDPR-prescribed level of 4% of annual worldwide corporate turnover or €20 million, whichever is higher) and/or penalties, the suspension of cross-border data flows, the withdrawal of privacy certifications, and the (temporary or permanent) prohibition, freezing, or restriction of certain processing activities.

The Act repeals and supplements the procedural provisions in the current Belgian data protection legislation from 1992, which did grant certain enumerated powers to the Privacy Commission but did not contain specific rules of procedure. By enacting procedural provisions, the new Act formalizes the functioning of and interaction with the DPA as a law enforcer. Based on the explicit inclusion of the sanctions in the Belgian implementing Act, it is safe to assume that Belgium is getting ready to exercise the full range of administrative powers granted under the GDPR.

Different Legislative Approach Compared to Other Member States

A draft version of the Act was introduced in the Belgian Parliament on August 23, 2017. It enjoyed a speedy adoption just over two months later via expedited adoption procedures, with final publication of the adopted text appearing on November 16, 2017. Somewhat surprisingly, the text only addresses the structure of the Belgian DPA and its powers and does not address any of the various other areas where the GDPR allows for or requires national implementation (such as, for instance, the restriction of individual rights due to public interests or rules for processing employee data). Therefore, it is realistic to assume that Parliament will soon start preparing subsequent legislative proposals dealing with the remainder of GDPR implementation. The Act itself also suggests this because it expressly states that it only repeals the current Belgian Data Protection Act's sections on the structure and organization of the Privacy Commission (thus leaving the remainder of the provisions in place). Since the remainder of these provisions are not necessarily in line with the GDPR, further legislative action will be necessary to align Belgian privacy legislation with GDPR rules. The new Act should enter into force on May 25, 2018 (simultaneously with the GDPR); however, the Act allows for exceptions to this date. These include, for instance, provisions regulating the actual creation of the DPA since the DPA is expected to be fully operational as of May 25, 2018, which requires some advance planning and set-up (see, for example, Chapter III of the Act permitting early designation of members of the DPA's executive committee, knowledge center, and dispute resolution chamber). These provisions will be effective as of the date the Act was published in the Belgian Official Gazette (*Belgisch Staatsblad*) to allow for a timely establishment of the DPA by May 25, 2018.

It is remarkable that of the three member states that have already adopted GDPR implementation statutes, none have opted for a similar legislative route. When other member states included DPA-specific language, it was done as one part of a larger systematic statute alongside further sections implementing the GDPR's substantive provisions. By adopting legislation establishing a procedural framework *before* addressing substantive provisions, and by doing so via legislative text that introduces a great level of procedural detail, Belgium seems to set the tone of solid enforcement here.

International Cooperation

The Act supports international cooperation efforts and obligations of the DPA, which may exist in (1) the introduction of expert pools to allow for efficient information exchange; (2) mutual assistance in light of corrective measures and monitoring; and (3) the sharing of personal and financial means. Such cooperation may be supported by cooperation agreements. In light of international treaties, the DPA may also appoint specific members to act as representatives with international authorities, to the extent that they exercise powers within the competencies of the DPA.

A Solid Structure Inspired by Other Belgian Supervisory Authorities

The Act's reform of the DPA's structure is prompted by this significant increase in powers as the DPA goes from being a predominantly advisory body to a true investigatory and corrective authority. The six newly instituted agencies are structured in light of this and include an executive committee, general secretariat, frontline service, knowledge center, inspection body, and dispute resolution chamber. Each agency is free to seek advice from independent

experts where they deem fit, who in turn issue nonbinding opinions. In addition, the DPA will be assisted by an independent "reflection council" taking on what is in essence the same advisory role, but which will now be exercised internally within the DPA. The reflection council is composed of actors from across Belgian society in hopes of issuing multidisciplinary opinions.

The inspiration for this new DPA structure was found in – as the Act refers to it – "supervisory authorities with comparable powers" such as the Belgian Institute for Postal Services and Telecommunications and the Belgian Competition Authority, both of which have expansive competencies when it comes to investigations, administrative fines, and penalties.

The specific function of each agency in the new DPA is set forth in the Act. The executive committee ("*directiecomité*") is responsible for the general policy and day-to-day administration of the DPA, including administering the annual budget. It is composed of the presidents of all other agencies and chaired by the president of the DPA. Each year, it drafts the DPA's "strategic plan," which is put forth for public consultation. It also establishes the DPA's "internal code of conduct," which lays down certain rules that could have significant impact. The general secretariat ("*algemeen secretariaat*"), on the one hand, has purely clerical functions (receipt of complaints, administration of internal and external communications, etc.), but will also exercise several more substantive powers, such as approving internal codes of conduct, approving model clauses and binding corporate rules (BCRs), and preparing of a list of data processing activities requiring a data protection impact assessment (DPIA). The knowledge center ("*kenniscentrum*"), in its turn, will take on what is now the core function of the Privacy Commission, namely the issuance of guidance and recommendations in the field of data protection. Finally, the frontline service ("*eerstelijnsdienst*") acts as a "filter" to the dispute resolution chamber for any complaints that are filed. It is also the first point of contact between the DPA and external stakeholders (such as individuals or data controllers and processors), and can provide them with guidance or recommendations.

Establishment of Inspection Body and Dispute Resolution Chamber

The most significant bodies introduced by the new Act are the inspection body ("*inspectiedienst*") and the dispute resolution chamber ("*geschillenkamer*"). These two bodies transform Belgium's prior advisory commission into a true enforcement agency with monitoring and corrective powers.

Similarities to criminal investigations

The detailed outlines of procedural rules the Act establishes, and the measures it places at these agencies' disposal, are reminiscent of measures one would typically find in criminal investigations. The DPA inspection body, for instance, is composed of inspectors and led by an inspector-general ("*inspecteur-generaal*"). Its powers include the interrogation and written examination of individuals, on-site investigations, the consultation of IT systems and copying of relevant data, the seizure or sealing of assets or IT systems, and summoning the identification of the subscriber or regular user from a telecoms operator. In addition, the rights granted to individuals subjected to an interrogation are reminiscent of the rights usually present when law enforcement carries out criminal interrogations (notably the right to counsel, the right to obtain a free copy of interrogation transcripts, and the right to request performance of specific investigatory acts). The inspection body can also impose preliminary measures, such as temporarily suspending, restricting, or freezing processing activities, so that cases before the DPA could have major business impacts even in their investigatory phase. When exercising these powers, the inspection body may request the assistance of law enforcement when it deems it necessary. The investigatory phase remains strictly confidential up until the moment the inspector-general's report is filed with the dispute resolution chamber.

Far-reaching powers of the DPA

The Act's enforcement ambitions are further reflected by the scope investigations could potentially grow to. Individuals and entities subject to investigation are under a legal *duty of cooperation*, which the Act's Explanatory Memorandum compares to the duty of cooperation applicable to investigations by the Financial Services and Markets Authority (FSMA). Individuals and companies are required to hand over all information (save privileged information) that may serve to establish a data protection violation. The DPA bears a potentially light burden in justifying its opening of an investigation; more often than not, the DPA can exercise its powers "whenever it is deemed *necessary*," with the DPA in charge of determining that a particular exercise of power is "necessary" under the circumstances. Also important to note is that DPA investigators are not public prosecutors or members of police forces and may not be subject to the same safeguards Belgian statutes and practices have created for these investigatory institutions. The specific qualifications DPA investigators must possess are determined by the DPA's internal code of conduct, which is drafted by the DPA itself.

Sanctions taken by the dispute resolution chamber

The dispute resolution chamber is the final step in the DPA's administrative procedure path, and it is the body empowered to impose sanctions. It is an administrative body competent to exercise the so-called "corrective powers" granted to supervisory authorities under the GDPR. Its specific structure and organization strongly resemble a judicial institution or body, or Article I courts within the U.S. It is composed of a president and six members, all of whom are selected to ensure knowledge of data protection, administrative procedure, information security, and information and communications technology. The chamber's most significant corrective powers exist in the issuing of warnings and reprimands, the ordering of compliance with data subjects' individual rights requests, the temporary or definite freezing or restricting of processing activities (or a ban on the processing altogether), enjoining processing to be brought into compliance with data protection laws, imposing penalties and administrative fines, suspending cross-border data transfers, revoking privacy certificates, and publishing its decisions on its website. In terms of potential sanctions, the Act does not deviate from the GDPR.

Rules of Procedure

The Act's rules of procedure aim to enhance the effective protection for individuals' privacy rights, as well as regulating rights of defense and means of legal redress before the DPA and the regular civil courts. A procedure before the DPA is typically initiated by a request or complaint, but may also be initiated by the DPA on its own initiative in a number of situations. The rule for complaints and requests is that any individual, *as well as* associations and institutions, have legal standing to file. Here, Belgium seems to have taken advantage of the margin of manoeuver the GDPR grants member states to permit representative bodies to autonomously bring actions directly against regulators, controllers, or processors—i.e. without an individual's mandate. Because privacy or data protection rights are by default only conferred on natural, and not legal, persons, it is somewhat surprising that the GDPR—and now seemingly also the Belgian Act—would allow for legal persons (such as consumer organizations) to bring actions based on privacy violations without requiring a mandate from the person(s) actually granted this right. Beyond doctrinal considerations, allowing representative bodies to autonomously initiate data protection investigations/proceedings significantly increases the chance that companies will be faced with some form of data protection scrutiny. Unlike most individuals, professional representative bodies are less likely to be intimidated by administrative hurdles or long proceedings.

Frontline service

All complaints and requests are filed with the DPA's frontline service, which will conduct preliminary triage and decide on the admissibility of complaints and requests. Admissible complaints are transferred to the dispute resolution chamber, which can lead to either an investigation by the inspection body or, if the chamber decides sufficient evidence is available, administrative proceedings before the chamber itself. Information or other requests to the DPA are handled by the frontline service itself, which provides the requestor with the necessary information. Alternatively, the frontline service may also decide to initiate mediation to try and find common ground between both parties. If no solution is found in mediation, requests are treated in the same way as complaints and will be transferred to the dispute resolution chamber. Note that an inadmissibility decision by the frontline service may be appealed.

Inspection body

The "intermediary" chain in the procedure is the inspection body, which is responsible for conducting investigations to secure sufficient evidence for proceedings on the merits before the dispute resolution chamber. The inspection body can open an investigation in a number of different situations: (1) by request of the executive committee in the case of serious indications of a data protection law violation, in the context of a cooperation request form another supervisory authority, or when a case is brought to the DPA is by a judicial authority or administrative body; (2) by the dispute resolution chamber looking to gather more evidence in light of a complaint referred to it; or (3) upon its own initiative, again in the case of severe indications of a data protection law violation. The inspection body is also competent to impose preliminary measures (with a maximum duration of six months) when this is necessary to prevent an irreparable harm to the rights of the individual.

Note that the GDPR only foresees such measures in the case of a transnational processing activity, or in light of cooperation efforts of supervisory authorities—but the Belgian Act does allow for the imposition of such measures in *every* case pending before the inspection body. In light of procedural options, it is important to note that the defendant, after having been confronted with a preliminary measure, may request to be heard, file written or oral objections, and—most importantly—file an appeal against the measure with the dispute resolution chamber. The appeal, however, does not suspend the challenged measure (unless the chamber so orders), which raises questions about the practical impact or use of this procedural move. To prevent this, we recommend parties specifically request measures to be suspended until a final decision has been obtained in appeal (i.e., that the decision is "*niet uitvoerbaar bij voorraad*").

Dispute resolution chamber

The final chain in DPA procedure is the dispute resolution chamber, which will decide the case on the merits, meaning finding facts and imposing appropriate sanctions. Recapitulating, it can open a case directly via forwarding of matters by the frontline service, via the inspection body upon completion of the investigation phase, or at the level of appeal against a preliminary measure imposed by the inspection body. In principle, proceedings before the dispute resolution chamber are written, though the chamber may decide to organize oral hearings. Note that proceedings before the dispute resolution chamber will continue even when the defendant does not file a defense or when he/she does not respond to a request to appear before the chamber. The procedure before the chamber can take two turns: either the chamber decides to request (additional) investigation from the inspection body, or it decides to follow a "summary procedure" in which it treats the complaint autonomously without consulting the inspection body.

The latter option goes hand in hand with very limited notifications to parties involved in the proceedings—which may significantly reduce procedural options. If an investigation is requested, parties are generally offered a broad range of procedural safeguards, such as appropriate notifications, the filing of a defense strategy, the right to have all relevant exhibits attached to the file, and the right to be heard.

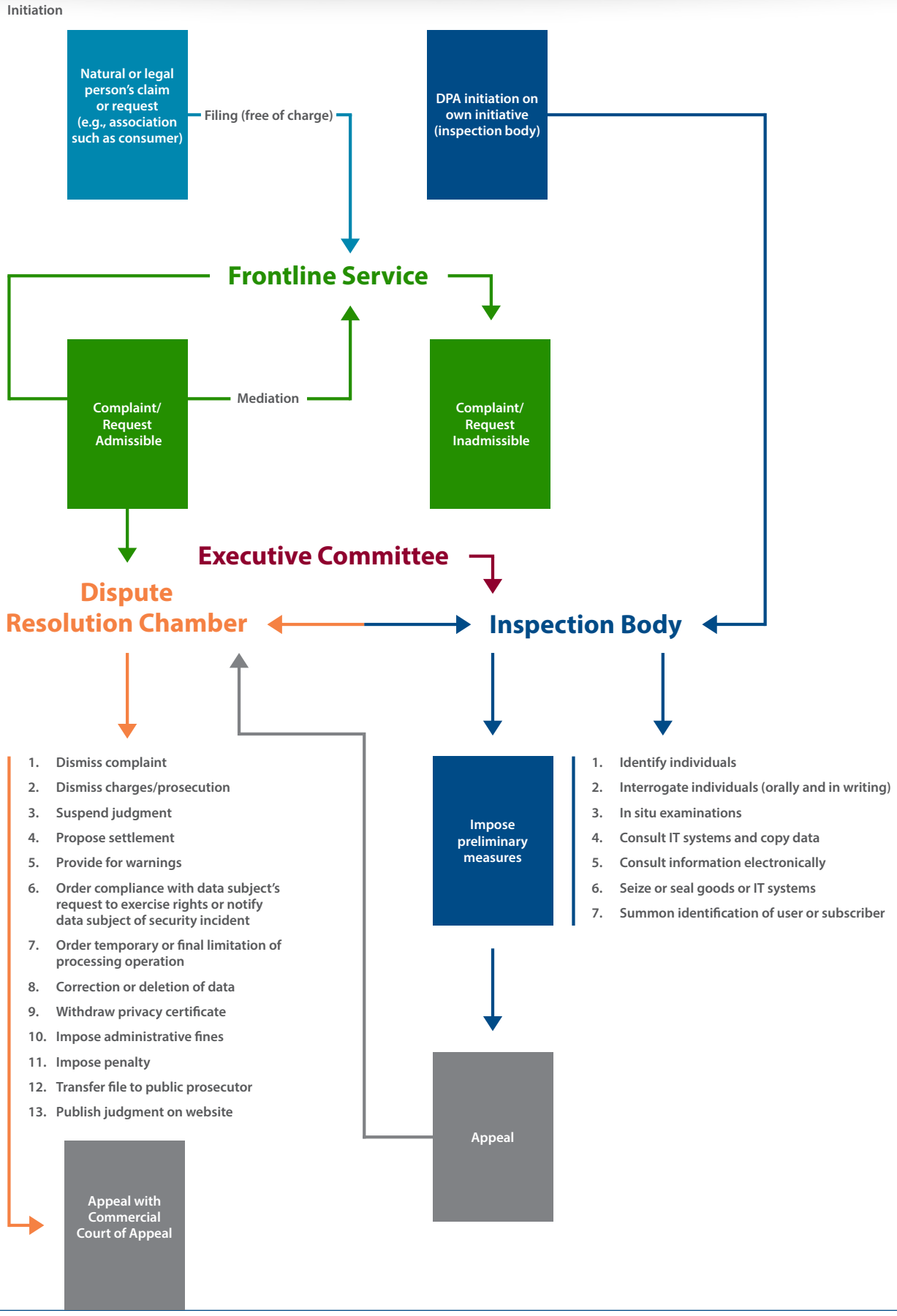
Administrative sanctions accumulation

Since the sanction mechanism provided for in the GDPR is often compared to sanctions foreseen in EU competition law (the equivalent of U.S. antitrust laws), it is key to understand the level of sanctions or fines that could potentially be imposed by national supervisory authorities. The Act distinguishes the level of the fine payable in situations where *several* distinct acts lead to multiple violations and in cases where *one and the same* act infringes several data protection law provisions (for instance, due to a common core of fact able to be qualified as multiple violations). It is only in the latter case that *only one* fine applies: the highest administrative fine. In the former case, administrative fines will be *added up*, subject to a cap at the level of the "highest administrative fine *times two*."

Appeal

As soon as the dispute resolution chamber renders a decision, the parties may file an appeal within 30 days with the Commercial Court of Appeal ("*Marktenhof*"), which will deal with the case in accelerated proceedings on the merits ("*zoals in kort geding*") to allow for timely judicial relief. The Commercial Court of Appeal was instituted following a legislative reform in Belgium at the beginning of this year to treat all appeals against regulatory agency decisions (which often require particular expertise). However, decisions taken by the dispute resolution chamber are "executable notwithstanding appeal," meaning the losing party cannot (preliminarily) escape sanctions using the escape route of suspensive appeal proceedings—unless, of course, the Commercial Court of Appeal orders otherwise. Parties faced with negative decisions imposing sanctions must be prepared and take the necessary precautionary measures to be able to execute the decision. In the same way, a decision from the dispute resolution chamber establishing a violation of data protection law can serve as a basis for the individual plaintiff to bring a damages claim before the competent civil court.

Outline of Procedure Before the Belgian DPA



You can subscribe to future *Privacy & Data Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Dominique R. Shelton
213.576.1170
dominique.shelton@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Jeffrey E. Tsai
415.243.1015
213.576.2608
jeff.tsai@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Michael Zweiback
213.576.1186
202.239.3186
michael.zweiback@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM