

Data Privacy & Protection

AZB & Partners boasts a highly specialized and diverse Data Privacy & Protection team comprising EU GDPR certified members, industry body representatives and sector-wise experts, adept in handling domestic and cross-border advisory and transactional matters. Our specialists hail from a number of practices, including TMT, FinTech, Healthcare and IP, which allows us to render advice tailored to the regulated space within which our clients operate. Our team demonstrates considerable sectoral expertise in healthcare, IT, e-commerce, blockchain, AI, automotive, electronics and financial and payment technologies.

Our work includes:

- Advocacy and public policy engagements, including participating in stakeholder consultations on the evolving data privacy and protection framework
- Assisting clients with developing a 'play book' on dealing with cyber-attacks and data breaches, including risk mitigation strategies
- Drafting privacy policies, data retention policies and archiving policies
- Advising on consent related requirements for the collection and transfer of personal and sensitive data and data localization requirements
- Advising on privacy related challenges and compliance requirements arising from the adoption of new technologies
- Advising clients on 'cyber security incidents' and data breaches, including reporting to CERT-In



Tata on the privacy and data protection aspects of the (i) storage, management and transfer of subscriber data for digital customer programs and payment facilities; and (ii) handling and transfer of subscriber data for vehicle technologies, card vault technologies and M2M business.



Amazon on (i) the data protection framework applicable to its marketplace and e-commerce business, AI applications, devices and programs, testing, health and COVID-19 preparedness and payments and cloud business; (ii) applicable data localization requirements; and (iii) privacy by design frameworks.



Tremco Incorporated on data privacy laws in India relating to its (i) agreement with a payroll service provider; and (ii) terms and conditions for the use, storage and handling of employee related sensitive personal data.



Star India on (i) content liability issues under the Information Technology Act, 2000; and (ii) preparing the privacy policy and terms of use for its website, 'www.hotstar.com' and associated mobile applications.



Canada Pension Plan Investment Board on data privacy laws relating to its terms and conditions for the use, storage and handling of employee related sensitive personal data.



Samsung India Electronics on issues relating to the notice requirements for its collection, handling, disclosure and transfer of personal information, including sensitive personal data or information.



Bank of America on (i) data protection and privacy regulations relating to the banking business; and (ii) the validity of e-signatures and electronic contracts.



Dream 11 on (i) drafting and preparing the privacy policy for its online fantasy gaming website; and (ii) applicable data privacy laws in India.



Aegon Life Insurance Company on (i) liability issues associated with a 'data breach,' and (ii) reporting requirements under the Information Technology Act, 2000.



NBA Asia on its privacy policy for the Junior National Basketball Association Program, in accordance with the data privacy regulations in India.



Toyota Motors with respect to privacy considerations relating to the launch of vehicle technologies.



J.P.Morgan on applicable data privacy laws in relation to its global data processing and outsourcing centers in India.



Montblanc on data privacy laws in the context of its privacy statements and policies for customer cards.



Bharti Airtel on (i) data sharing strategies; and (ii) establishing a framework for its digital business.



Dell on setting up and aligning its data protection and cybersecurity framework across business verticals.