BCLP. Client Intelligent

TECHNOLOGY TRANSACTIONS

OVERVIEW

All businesses have digital and technology strategies, irrespective of sector or geography. BCLP has a fully integrated, global team that lives and breathes the full range of transactions that affect our clients' digital and technology transactions, supporting them on their most complex and strategic cross-border projects. We take a resolutely business-oriented and outcomes-based approach. We tell our clients what is market to achieve a more efficient process. We also add value by spotting the critical and risk issues that impact the bottom line, which means we are constantly concentrated on our clients' strategic goals.

At BCLP, we deploy the right lawyers for the relevant technology subsector that is key to the client's needs, from fintech and payment solutions to AI and other advanced technologies; from digital media to mobile communications, across all service lines in our global firm. See the related subsector pages for greater detail on our experience in these areas.

We represent clients from investors (VCs, corporates and PE) and technology businesses (from startups and high-growth to mature companies) to enterprise users (including corporates and financial services institutions procuring or investing in technology) advising on all aspects of their transactional activity or disputes.

Our clients operate across all sectors of the global economy, spanning financial services including payments, telecommunications, media and advertising, real estate, energy and infrastructure, retail, hospitality, sports and health care.

DIGITAL SPEAKS SERIES

'Digital Speaks Series', BCLP's Knowledge Platform

Explore key topics affecting the digital world, including AI, Cloud, data privacy and security, digital assets/blockchain, the digital disruption in sports and entertainment, ESG, regulation of 5G/6G and many more.

MEET THE TEAM

Marcus Pearl

Partner and Global Practice Group Leader – Technology, Commercial & Government Affairs, London

marcus.pearl@bclplaw.com
+44 (0) 20 3400 4757

AREAS OF FOCUS

- PropTech
- AdTech
- Software, Cloud Subscription & Systems Integration
- Software Audits
- Digital Transformation & Emerging Technology

RELATED INSIGHTS

News
Apr 30, 2025
BCLP advises SatixFy on the English law aspects of its proposed acquisition by MDA Space

Insights
Apr 29, 2025
Understanding DORA: a guide for financial entities and ICT service providers

Blog Post
Dec 09, 2024
President-elect Trump's Pick to Lead DOJ's Antitrust Division Signals Continued Aggressive Big Tech and Agriculture Enforcement

Insights
Dec 06, 2024

What is the impact of the EU's new Network and Information Systems Directive for Businesses?

Forming part of the EU's broader digital and cyber security strategy, the new Network and Information Systems Directive 2022/2555 (NIS2) came into effect on 18 October 2024 (this being the deadline by which the directive is required to be implemented into national law, although this process is not yet complete). It replaces NIS Directive 2016/1148 and complements the EU's Cyber Resilience Act (discussed in a recent BCLP insight). The revised directive is intended to cast a wider net and bring more industries and sectors directly within its regulatory remit. In-scope businesses will therefore need to ensure appropriate risk-management procedures are embedded across their organisations. Senior management also need to understand the oversight which they are required to exercise, given the personal liability for cybersecurity failings which NIS2 now mandates.

Insights
Nov 25, 2024

Key insights on the EU Cyber Resilience Act – what businesses need to know

The Cyber Resilience Act (CRA) is a groundbreaking piece of legislation designed to enhance the cybersecurity of digital products and services made available in the EU. Published last week in the Official Journal of the European Union, it marks the start of a phased 3 year implementation period. The CRA aims to strengthen the resilience of the EU's digital economy by imposing stricter requirements on manufacturers, importers, and distributors of products or software with a digital component and will therefore have significant compliance consequences for businesses.

Insights
Nov 25, 2024

Managing technology supply chains

The FCA, PRA, and Bank of England have published their finalised critical third party (CTP) rules (and accompanying guidance) in PS24/16 Operational resilience: Critical third parties to the UK financial sector.[1]The new rules, which come into force on 1 January 2025, will see designated technology providers whose failure is deemed to pose a systemic risk to the UK financial system become subject to new principles-based, outcomes-focused rules and requirements overseen by the financial services regulators. This is timely given the increasing trend in third-party related incidents affecting operational resilience at financial services firms. On 31 October, the FCA published its "lessons for operational resilience" following its review of the financial services sector's response to the recent CrowdStrike outage, which noted that third-party related issues were the leading cause of operational incidents reported to …

Insights
Sep 20, 2024

The EU's Digital Operational Resilience Act 2022/2554 (DORA)

News
Sep 17, 2024

BCLP advises Playtech plc in connection with the proposed sale of Snaitech S.p.A. for a total enterprise value of EUR€2.3 billion

BCLP has advised client Playtech plc (Playtech), in connection with the proposed sale of Snaitech S.p.A. (Snaitech) to Flutter Entertainment Holdings Ireland Limited, a subsidiary of Flutter Entertainment plc (Flutter), for a total enterprise value of EUR€2,300 million in cash.

Insights
Sep 03, 2024

AI Surveillance and Data Privacy at the Games

As the Paris 2024 Summer Olympic and Paralympic Games (the “Games”) turn onto the final straight, the Games have yet again captured widespread global attention, on and off the track. With over 15.3 million visitors in Paris this summer for the Games, data security has emerged as a critical concern. To enhance the safety of athletes, spectators and residents, the French government implemented specific measures, including a bill relating to the Games (the “OG law”), a legislative measure passed on 19 May 2023, to bolster security during the Games[1]. The “OG law” introduces advanced security measures, notably the use of experimental algorithmic video surveillance systems. This article focuses on the deployment of these augmented surveillance systems during the Games and examines the associated GDPR compliance and privacy dilemmas that subsequently arise.