

# Bird & Bird & Cryptography Transfers

*Cryptography driven technology and software have become part of our daily routine found in numerous products, applications, (security) solutions and services. At the same time, sharing and transferring such software and technology is not without any measure of constraint. Numerous governments monitor and control transfer of cryptography for (inter)national security, national cryptography, trade or foreign policy interests and objectives. Due to the rise of the digital economy, digital transformation and telecommuting, this is becoming an area of increasing regulatory interest and enforcement. Any non-compliance can lead to severe penalties, even personal liability.*

## What type of transfer?

Each country has its own national cryptography policy and regulatory framework controlling certain type of transfer activity.

Types of transfers being regulated can involve any of the following activities:

- Supply
- Import
- In-country transfer and/or download
- Intra-EU Member States transfer
- Export

The national regulatory frameworks can control tangible as well as intangible transfers (e.g. electronic transfers such as e-mails, cloud computing, open source community, etc.).

## Different countries, different rules

The legal and regulatory requirements regarding cryptography transfers differ per country.

For each country, however, the main starting point is to have clearly identified whether your product, application, solution or service is using cryptography (or e.g. embeds activation of encryption functions) in order to be able to check the applicability and – if so – mandatory compliance regarding the transfer regulatory requirement in the country concerned.

In some countries, the scope and compliance regulatory requirements are moderate while, in other countries, burdensome and complex. We have extensive experience dealing with various governmental administrations having built strong relationships over the past years.

## Time to ask yourself...

Are you involved in cryptographic or encryption-based products, (innovative) solutions, applications or services?



Are you involved in cross-border transfers, intra-company transfers, import, in-country downloads, export?



Are you aware that encryption or cryptographic based products, (innovative) solutions, applications or services can be controlled subject to regulatory requirements in view of their transfer(s)?



Do you have a process in place to manage compliance and any potential risks?



Are you aware of the potential risks and liabilities?



Exposure to financial, criminal and/or incarceration liability risks, reputational damage or the inability to operate in key markets impacting the performance of your business, its financial statements and ability to achieve its strategic objectives



Having doubts, feel free to request our *CryptographyTransferScan*

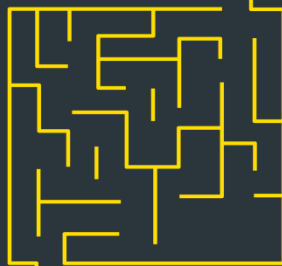
## Our key experience:

- *Advising a multinational computer software and technology developer regarding the applicability and enforcement of import and export encryption controls in view of licensing, cross-border asset purchase agreements, software licensing agreements and day-to-day cross-border sales and transfers of encryption software and related source code to various countries. We incorporated encryption controls compliance manuals, evaluated contractual clauses as well as performed a risk and liability assessment of past sales, supplies and transfers regarding encrypted products.*
- *Advising an American multinational investment bank and financial services company regarding encryption controls and related licensing for the import of encryption based mobile authenticators in various third countries.*
- *Advising a global artificial intelligence company regarding the import encryption controls for its platform software for artificial intelligence and machine learning technologies.*
- *Advising an international cyber security and privacy company regarding encryption controls regarding of its secure storage mobile applications as well as submitting successful voluntary self-disclosure regarding past violations to the competent authority.*

## Our global main contact:

Goran Danilović  
Lawyer/Advocate

Tel: +31 (0)70 353 88 78  
[goran.danilovic@twobirds.com](mailto:goran.danilovic@twobirds.com)



twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw & Satellite Office: Casablanca

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.