PANORAMIC

FINTECH

Netherlands

LEXOLOGY

Fintech

Contributing Editors

Angus McLean and Oliver Irons

Simmons & Simmons

Generated on: October 2, 2024

Contents

Fintech

DATA PROTECTION AND CYBERSECURITY

OUTSOURCING AND CLOUD COMPUTING

INTELLECTUAL PROPERTY RIGHTS

COMPETITION

TAX

IMMIGRATION

UPDATE AND TRENDS

Contributors

Netherlands

Simmons & Simmons

Jeroen Bos	jeroen.bos@simmons-simmons.com
Koen van Leeuwen	koen.vanleeuwen@simmons-simmons.com
Sophie Wesselink	sophie.wesselink@simmons-simmons.com

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

What is the general state of fintech innovation in your jurisdiction?

Fintech innovation in the Netherlands continues to develop. There has been a high level of activity in the fields of artificial intelligence, machine learning, blockchain, mobile and advanced analytics. The Dutch market has also been at the forefront of adopting other innovations such as open banking (as a result of Directive (EU) 2015/2366 (second Payment Services Directive)).

Generally, diversification in the Dutch financial services sector has increased due to new entrants entering the market and incumbents (such as large Dutch banks) progressing their own fintech initiatives. However, increasing regulatory scrutiny and supervisory costs seems to deter new entrants into the market. Nevertheless, despite the additional administrative and compliance costs of the Dutch registration regime for certain crypto service providers that applies since May 2020, over 50 crypto service providers are registered to date.

Law stated - 1 June 2024

Government and regulatory support

Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In June 2016, the Dutch Authority for the Financial Markets (AFM) and the Dutch Central Bank (DNB) set up the InnovationHub to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services. The InnovationHub is a joint information desk of the AFM, the DNB and the Dutch Authority for Consumers and Markets (ACM). It aims to offer easy access to supervisors and regulators for companies that provide innovative services or products, gain more insight into the rapidly developing technological innovation within the financial sector, and improve knowledge, sharing and dialogue with all relevant stakeholders. Firms can submit specific questions through the Innovation Hub, to which the DNB, the AFM and the ACM provide informal answers.

In 2016, the AFM and the DNB set up the Regulatory Sandbox for fintech companies to test and develop new products. If certain criteria are met, the Regulatory Sandbox can provide bespoke solutions for financial services companies that cannot reasonably meet specific policies, rules or regulations when marketing an innovative product, service or business model, but that do meet the underlying rationale of these policies, rules or regulations. The Regulatory Sandbox was evaluated as part of the discussions taking place in the iForum.

The DNB also periodically organises the Fintech meets the Regulator seminar, during which relevant market participants and the DNB share thoughts on current developments.

Additionally, in November 2019, the DNB launched the iForum, a platform for joint initiatives intending to create value for the Dutch sector and the DNB. Through the iForum, the Dutch sector and the DNB can have a dialogue on the impact of technological innovations on the sector and develop joint pilots and experiments.

In October 2021, the ACM, the AFM, the Dutch Data Protection Authority (AP) and the Dutch Media Authority (CvdM) established the Digital Regulation Cooperation Platform (SDT). The SDT wishes to gain more insight into the online use of personal data by algorithms, among other things, and will coordinate how to enforce (new) EU rules and regulations on digitalisation. For example, this includes new rules and regulations on dealing with large technology companies, the data economy and the platform economy (such as the Digital Services Act, the Digital Markets Act, the Data Governance Act and the Artificial Intelligence Act).

There are no formal arrangements with foreign regulators that relate specifically to fintech companies. However, both the AFM and the DNB maintain contact with other regulators in the Netherlands (such as the ACM, the AP and the CvdM), the European Union and globally (such as the International Organization of Securities Commissions).

Law stated - 1 June 2024

FINANCIAL REGULATION

Regulatory bodies
Which bodies regulate the provision of fintech products and services?

There is no specific regulatory framework applicable to the provision of fintech products and services, besides the registration regime for certain crypto service providers. Such crypto-service providers are supervised by the Dutch Central Bank (DNB).

As such, depending on the nature and scope of fintech products and services offered, these are regulated by the Dutch Authority for the Financial Markets (AFM) or the DNB, or both, which supervise compliance with the conduct of business rules and prudential requirements respectively.

Law stated - 1 June 2024

Regulated activities
Which activities trigger a licensing requirement in your jurisdiction?

Depending on the nature and scope of services offered, licensing requirements under the Dutch Financial Supervision Act (FSA) and secondary legislation may apply.

Among others, the following activities are regulated under the FSA:

- deposit-taking and extension of credit for one's own account: credit institutions (ie, institutions that attract repayable funds from the public in the Netherlands and that extend credit for own account) require a banking licence;
- consumer lending: the extension of credit to consumers (natural persons acting outside their business or profession) requires a licence;
- factoring, to the extent this would constitute consumer lending, requires a licence;
- invoice discounting, to the extent this would constitute consumer lending, requires a licence;

- payment services: all persons providing payment services as described in the Annex to Directive (EU) 2015/2366 (the revised Payment Services Directive) (PSD2), require a licence. A licence to act as a credit institution may also cover providing payment services;
- acting as a payment processing service provider requires a licence;
- issuance of electronic money requires a licence;
- intermediation activities in respect of financial products require a licence;
- investment services: a person is required to have a licence for the provision of investment services. These can be split into the following services, carried out in pursuit of a business or profession:
    - receiving and transmitting client orders relating to financial instruments (which includes bringing about deals in financial instruments);
    - executing client orders relating to financial instruments;
    - managing an individual's assets;
    - providing advice regarding financial instruments;
    - underwriting or placement with a firm commitment basis of financial instruments; and
    - placement without a firm commitment basis of financial instruments;
- investment activities: a person is required to have a licence if it intends to perform an investment activity. Investment activities can be split into three activities:
    - dealing on one's own account (including foreign exchange trading);
    - operating an organised trading facility; and
    - operating a multilateral trading facility;
- clearing and settlement: acting as a clearing and settlement institution requires a licence;
- secondary market loan trading, to the extent this would constitute consumer lending, requires a licence;
- the managing of and offering units in an alternative investment fund or undertaking for collective investment in transferable securities requires a licence;
- conducting the business of a depositary requires a licence;
- offering investment objects requires a licence; and
- conducting the business of a (re)insurer requires a licence.

The registration regime for certain crypto service providers follows from the Dutch Money Laundering and Terrorist Financing (Prevention) Act. This regime only applies to crypto service providers that provide exchange services between fiat currencies and virtual currencies and (or) provide custodian wallet services for virtual currencies in or from the Netherlands.

Law stated - 1 June 2024

Consumer lending

Is consumer lending regulated in your jurisdiction?

Under the FSA, consumer lending requires a licence. Consumer credit is considered a financial product. Advising a consumer on a financial product or providing intermediary services in relation to such a financial product is only permitted if the institution has obtained a licence from the AFM. Financial institutions may be exempted if they have another licence that permits consumer lending or advising consumers on financial products.

Before entering a loan agreement with a consumer, the financial institution must provide the consumer with relevant information relating to the financial product, so that the consumer is able to properly assess the product. In addition, credit assessment rules exist to prevent consumer over-indebtedness. These rules are part of the overarching requirement that lenders exercise due care when providing these services.

Law stated - 1 June 2024

Secondary market loan trading

Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is only a regulated activity where it constitutes consumer lending.

Law stated - 1 June 2024

Collective investment schemes

Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In the FSA, collective investment schemes can be an alternative investment fund, as defined in Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD), or an undertaking for collective investment in transferable securities, as defined in Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive (UCITSD).

Under the AIFMD, an alternative investment fund is a vehicle with or without legal personality, which raises capital from investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors. The AFM has confirmed that firms managing or offering units in funds that invest in cryptocurrencies require a licence as an AIFM.

Whether a fintech company qualifies as a collective investment scheme depends on the exact nature of its business. For example, fintech companies that manage assets on a pooled basis on behalf of investors should give particular consideration as to whether they qualify as a collective investment scheme. On the other hand, fintech companies that provide

advice or payment services may be less likely to constitute a collective investment scheme. Peer-to-peer lenders, marketplace lenders or crowdfunding platforms could potentially fall within the scope of the AIFMD, to the extent they would qualify as (managers of) collective investment schemes.

Law stated - 1 June 2024

Alternative investment funds

Are managers of alternative investment funds regulated?

Yes. Managers of alternative investment funds are regulated under the AIFMD, which has been implemented in the FSA.

Law stated - 1 June 2024

Peer-to-peer and marketplace lending

Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There is no specific regulation of peer-to-peer (P2P) or marketplace lending in the Netherlands. However, this activity might constitute a regulated activity under the FSA. For instance, if a platform facilitating P2P lending receives and transmits orders in financial instruments, it may be subject to a licensing obligation as an investment firm.

Law stated - 1 June 2024

Crowdfunding

Describe any specific regulation of crowdfunding in your jurisdiction.

As of 10 November 2021, the EU Crowdfunding Regulation applies. Among other things, this Regulation introduced a licensing regime for crowdfunding service providers (CSPs) that:

- facilitate granting of loans excluding consumer credit (loan-based crowdfunding); or
- place without a firm commitment basis transferable securities and instruments issued by project owners or SPVs, and receive and transmit orders for crowdfunding purposes (equity-based crowdfunding).

However, if crowdfunding offers made by a particular project owner exceed €5 million over a period of 12 months, then the licensing regime for investment firms under Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2) applies instead.

After the expiry of the (extended) transitional period on 10 November 2023, CSPs require a licence from the AFM for the provision of crowdfunding services.

Law stated - 1 June 2024

Invoice trading

Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation of invoice trading in the Netherlands. However, depending on the exact services provided and the status of the parties involved, invoice trading may lead to either party qualifying as an intermediary of consumer credit or may amount to the extension of consumer credit.

Law stated - 1 June 2024

Payment services

Are payment services regulated in your jurisdiction?

Yes. In the Netherlands, payment services are regulated based on PSD2, which has been implemented in the FSA. A licence is required to provide the payment services listed in Annex I to PSD2.

Payment services include:

- services enabling cash to be placed on a payment account or cash withdrawals from a payment account and all the operations required for operating a payment account;
- the execution of the following types of payment transactions:
- direct debits, including one-off direct debits;
- payment transactions executed through a payment card or a similar device; and
- credit transfers, including standing orders; and
- the execution of the following types of payment transactions where the funds are covered by a credit line for the payment service user:
- direct debits, including one-off direct debits;
- payment transactions executed through a payment card or a similar device; and
- credit transfers, including standing orders; and
- issuing payment instruments or acquiring payment transactions;
- money remittance;
- payment initiation services (initiating a payment order at the request of a payment service user with respect to an account held with another payment service provider); and
- account information services (online services to provide consolidated information on one or more payment accounts held by the payment service user with another one (or more) payment service provider).

Law stated - 1 June 2024

Open banking

Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The implementation in the FSA of the access-to-account rules, as included in the PSD2, requires financial institutions to provide access to the payment accounts of clients to payment initiation service providers and account information service providers. In general, data protection and privacy regulations should be considered prior to making client data available to third parties.

Law stated - 1 June 2024

Robo-advice

Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is no specific regulatory framework applicable yet to robo-advisers in the Netherlands.

As such, there is no legal distinction between robo-advice and traditional investment advice in the Netherlands. Therefore, companies providing robo-advice must – in principle – fulfil the same legal requirements as companies providing traditional investment advice.

However, as of 1 July 2024, certain requirements will apply to the provision of automated advice. These requirements aim to safeguard the adequate provision of automated advice. Financial service providers that provide automated advice on financial products should:

- designate one or more individuals that are responsible for the automated system and automated advice. These individuals should have the required knowledge and competences to advise on the relevant financial product themselves;
- conduct an analysis of the automated system before it is used to ensure that it works and all components of the advice are suitable for the client and periodically assess whether the provided automated advice is indeed suitable; and
- take certain measures in case the provided automated advice does not comply with the applicable rules and regulations. These measures include (temporarily) ceasing the provision of automated advice, checking the system to identify the error that has caused the non-compliance and inform the clients that have been affected by such error.

Furthermore, the AFM has issued two documents relating to robo-advice:

- the AFM's view on robo-advice, in which the AFM discusses the duty of care and points of attention specifically in relation to robo-advice on mortgage loans and occupational disability insurance (but also in relation to other high-impact financial products). In general, the AFM states that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider, including:
    - determining for which target group robo-advice is suitable;

- determining which financial products are included in the robo-advice;
- the algorithm's ability to identify when clients have doubts;
- detection of contradictory client answers; and
- explanations on the product features and advice; and

- guidelines for (semi)-automated portfolio management, in which the AFM provides guidance regarding the (technique-neutral) duty of care of asset managers who offer semi-automatic investment advice and portfolio management. These guidelines are not legally binding but they do bring clarity for asset managers. The guidelines are aligned with Dutch law, MiFID 2 and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

Also, in its guidelines on the qualification of innovative services, the AFM touches upon the automation of investment services and the impact thereof on the legal qualification of such investment services.

Law stated - 1 June 2024

Insurance products
Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. The sale of insurance products is regulated under the FSA and requires a licence.

Law stated - 1 June 2024

Credit references
Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The rules on credit rating agencies laid down in Regulation (EC) No. 1060/2009 on credit rating agencies (as amended) apply in the Netherlands. A credit rating agency is required to adopt, implement and enforce adequate measures to ensure that the credit ratings it issues are based on a thorough analysis of all the information that is available to it and is relevant to its analysis according to its rating methodologies.

Law stated - 1 June 2024

CROSS-BORDER REGULATION

Passporting
Can regulated activities be passported into your jurisdiction?

An EEA firm that has been authorised under one of the EU single market directives, such as (Directive 2013/36/EU (Capital Requirements Directive), Directive 138/2009/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Recast), Directive 2014/65/EU (Markets in Financial Instruments Directive II), Directive (EU) 2016/97 (Insurance Distribution Directive) (Recast), Directive 2014/17/EU (Mortgage Credit Directive), Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive, Directive 2011/61/EU (Alternative Investment Fund Managers Directive) and Directive (EU) 2015/2366 (revised Payment Services Directive) may, in principle, provide cross-border services into or establish a branch in the Netherlands.

This also applies to an EEA firm authorised as a crowdfunding service provider under Regulation (EU) 2020/1503 on European Crowdfunding Service Providers and will also apply to cryptoasset service providers authorised under Regulation 2023/1114 on Markets in Crypto-Assets.

To exercise this right, in general, the firm must first notify its home state regulator. The relevant directive (as implemented in the Dutch Financial Supervision Act) or the regulation under which the EEA firm is seeking to exercise its passporting rights will determine the conditions (if any) and processes that the EEA firm must follow.

Crypto service providers registered elsewhere in the EEA for the provision of exchange services between virtual and fiat currencies or custodian wallet services, or both, currently cannot passport their services into the Netherlands.

Law stated - 1 June 2024

Requirement for a local presence

Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

To obtain a licence for any of the activities regulated pursuant to the FSA; in general, a local presence must be established, unless a firm can benefit from a European passport or a specific cross-border licensing regime is available.

Law stated - 1 June 2024

SALES AND MARKETING

Restrictions

What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Depending on the regulatory status of the financial institution, different marketing rules may apply, including clientele restrictions. Advice should be sought on the specific circumstances of any particular case.

The Dutch Financial Supervision Act (FSA) states that, in general, relevant marketing activities:

- must be correct, clear and not misleading;

- must be recognisable as being of a commercial nature (where applicable); and
- may not contradict the information that is required to be made available pursuant to the FSA.

In addition, specific rules apply depending on the type of product offered or service provided and, in some cases, also on the type of client targeted. Some of these are summarised below.

Marketing materials for complex products (eg, participation rights in an open-ended collective investment scheme and investment objects) should include a risk indicator as prescribed by the Dutch Further Regulation on Conduct of Business Supervision of Financial Undertakings (the Further Regulation).

Marketing materials for credit offerings to consumers that refer to debit interest rates or other information regarding costs should include (at a minimum) information regarding floating or fixed interest rates and other costs that form part of the total costs of the credit for the consumer, the total credit amount, the yearly cost percentage, identity and address of the provider or intermediary, and certain other information depending on the type of credit, all as prescribed in the Decree on Conduct of Business Supervision of Financial Undertakings.

In addition, certain risk warnings are prescribed and certain prohibitions apply, such as the prohibition on including any references to the speed or ease with which the credit may be obtained.

For products other than complex products, general marketing rules included in the Further Regulation apply, including the obligation to include a warning that the value of an investment may fluctuate and that historical returns offer no guarantee for the future.

Depending on the medium used for marketing (print, TV, radio or internet) further rules apply, such as the relevant information to be included at a minimum (namely, the name of the provider, the regulatory status of the provider, and where and how further information relating to the product or service can be obtained). Specific marketing rules have been introduced to facilitate marketing on social media.

Furthermore, the Dutch Authority for the Financial Markets (AFM) has imposed a ban on the selling, marketing or distribution of binary options to retail clients. It has also imposed restrictions with respect to the selling, marketing and distributing of contracts for differences to retail clients and turbos to retail clients (with respect to contracts for differences and turbos, among others a leverage cap for such products with crypto as an underlying is imposed).

Finally, there is increasing attention from the AFM for the role of 'finfluencers' in promoting certain products or firms.

Law stated - 1 June 2024

CRYPTOASSETS AND TOKENS

Distributed ledger technology

Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Currently, no specific rules or regulations apply that govern the use of distributed ledger technology (DLT) or blockchain, other than Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology, which became applicable on 23 March 2023. This pilot regime lays down uniform requirements for firms that intend to operate a DLT infrastructure. DLT market infrastructures may only admit to trading or recording DLT financial instruments on a distributed ledger.

Firms that intend to operate under this pilot regime need to apply for a permission from the Dutch Authority for the Financial Markets (AFM) as a:

- DLT multilateral trading facility;
- DLT settlement system; or
- DLT trading and settlement system.

The pilot regime will, in any case, apply for a period of three years, after which an evaluation at the EU level will take place.

Generally, the use of DLT is subject to existing regulatory legislation (eg, the Dutch Financial Supervision Act (FSA)) depending on its application in any particular case. DLT is a topic that has led to many questions in the InnovationHub.

Law stated - 1 June 2024

Cryptoassets

Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Dutch Central Bank (DNB) and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies.

However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies. For example, this would be the case when the holder of a digital wallet is able to convert its digital currency holdings into cash holdings held with the crypto-service provider. Furthermore, depending on the structure and the specific characteristics of the digital currency or digital wallet, the relevant services could be considered to constitute payment services or e-money-related services. In these circumstances, unless an exemption applies, the relevant activities trigger a licence requirement under the FSA and certain prudential and conduct-of-business rules will apply.

Additionally, crypto service providers that provide exchange services between virtual and fiat currency or custodian wallet services in or from the Netherlands are required to register with the DNB.

On 29 June 2023, the EU Markets in Crypto-Assets (MiCAR) entered into force. MiCAR will apply to cryptoasset service providers as of 30 December 2024 and to issuers of asset-referenced tokens and e-money tokens as of 30 June 2024.

MiCAR intends to regulate assets and service providers that are currently out of scope of the regulatory perimeter. As of 30 December 2024, the current registration regime under the Dutch Money Laundering and Terrorist Financing (Prevention) Act will be replaced by the licensing regime for cryptoasset service providers under MiCAR.

Under MiCAR cryptoassets are categorised as e-money tokens, asset-referenced tokens and cryptoassets other than asset-referenced tokens and e-money tokens (including utility tokens). This categorisation also covers certain types of stablecoins.

Cryptoassets that are currently regulated (eg, as a financial instrument or e-money) will not fall within the scope of the MiCAR. Also, unique NFTs for now will not fall within the scope of the MiCAR (but fractional NFTs and large NFTs collections will fall within scope).

Further, MiCAR will regulate the provision of the following cryptoasset services:

- the provision of custody and administration services for cryptoassets;
- the operation of a crypto trading platform for cryptoassets;
- the exchange of cryptoassets for funds;
- the exchange of cryptoassets for other cryptoassets;
- the execution of client orders in cryptoassets;
- the placing of cryptoassets;
- the reception and transmission of client orders in cryptoassets;
- the provision of advice on cryptoassets;
- the provision of portfolio management on cryptoassets; and
- the provision of transfer services for cryptoassets.

Any legal person or undertaking providing these cryptoasset services in the course of the business to clients on a professional basis (cryptoasset service providers (CASPs)) is required to obtain a licence. For the Netherlands, the competent authority is the AFM, which opened its licensing application window on 22 April 2024. No simplified application procedure with the AFM will apply for crypto service providers that are currently registered with the DNB.

In principle, the licensing obligation for CASPs applies as of 30 December 2024. However, MiCAR provides for a transitional regime for CASPs that provided their services in accordance with applicable law before this date. This means that such already active CASPs – to the extent they are acting in accordance with national law – should be permitted to provide cryptoasset services without a MiCAR licence after 30 December 2024 during the transitional period.

In this context, MiCAR provides for a maximum transitional period of 18 months, giving the freedom to individual EU member states to apply a shorter (or no) transitional period. The Dutch legislator has confirmed its intention to apply a shorter transitional period of six months, which ends on 30 June 2025. As firms are not permitted to 'passport' under the transitional regime, they should ensure that they comply with the transitional period applicable in each EU member state in which they provide cryptoasset services, noting that the transitional period across these EU member states varies.

Both the Dutch legislator and the AFM have confirmed that only firms that are currently registered with the DNB are able to avail themselves of the transitional regime in the Netherlands. This means that only such registered crypto service providers can provide cryptoasset services in the Netherlands without a MiCAR licence until 30 June 2025.

In addition, MiCAR introduces a regime for the offering of cryptoassets to the public and the admission to trading on a trading platform of cryptoassets.

Law stated - 1 June 2024

Token issuance

Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The DNB and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies (unless these in specific circumstances do qualify as financial instruments). However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies.

Further, crypto service providers that provide exchange services between virtual and fiat currency (eg, by operating a crypto exchange) in or from the Netherlands are required to register with the DNB.

The AFM warned regarding the serious risks associated with ICOs, such as their vulnerability to misrepresentation, fraud and manipulation, their potential use for laundering money obtained by criminal means and the possibility that investors may lose their entire investment. In this context, the AFM advises customers to avoid investing in ICOs.

Furthermore, on 29 June 2023, the EU Markets in Crypto-Assets (MiCAR) entered into force. In respect of the offering of cryptoassets (other than asset-referenced tokens and e-money tokens) or admission to trading of such cryptoassets, MiCAR will apply as of 30 December 2024.

However, MiCAR will already apply as of 30 June 2024 in respect of the offering of asset-referenced tokens and e-money tokens and the admission to trading of these types of cryptoassets. This means that in principle issuers of such tokens should comply with the requirements under MiCAR as of that date, including but not limited to the publication of a white paper, licensing requirements, requirements on the content of market communication, internal organisational requirements and safeguarding arrangements.

That being said, MiCAR provides for a transitional regime under which issuers of asset-referenced tokens (other than credit institutions) that issued these tokens before 30 June 2024 are permitted to continue to do so until they have been granted (or refused) a licence under MiCAR, provided that they apply for such licence before 30 July 2024. Credit institutions that issued asset-referenced tokens in accordance with applicable law before 30 June 2024, may continue to do so until the cryptoasset white paper has been approved (or failed to be approved) provided that the required notification to their has taken place before 30 July 2024.

Law stated - 1 June 2024

ARTIFICIAL INTELLIGENCE

Artificial intelligence

Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Currently, there is no specific regulatory framework for the use of artificial intelligence (AI). Nevertheless, both the Dutch Central Bank (DNB) and the Dutch Authority for the Financial Markets (AFM) pay particular attention to the use of AI. For example, in 2019, the DNB published general principles for the use of AI in the financial sector. The DNB and the AFM focus on the use of AI in the insurance sector, by among others conducting market research. Further, in its report Machine Learning in Trading Algorithms, published in March 2023, the AFM reminds the market of the risks related to the use of machine learning in proprietary traders' trading algorithms. Additionally, on 9 April 2024, the DNB and the AFM jointly published a report on the impact of AI on the financial sector and supervision. In this report, the Dutch regulators discuss criteria and areas of attention for shaping the supervision of AI.

Also, on 29 May 2024, the European Council approved the Regulation on the use of AI (the EU AI Act). The EU AI Act will enter into force 20 days after publication in the Official Journal of the EU, and the publication is expected to take place in July 2024. In general, the EU AI Act will apply two years after its entry into force, so around mid-2026. Exceptions to this two-year timeline include the prohibition on banned AI systems (which will apply within six months of entry into force) and the governance rules and obligations for general purpose AI (which will apply within 12 months of entry into force).

The purpose of the EU AI Act is to promote the development and deployment of reliable and safe AI systems. The EU AI Act, among others, classifies AI systems at different risk levels, with high-risk systems being subject to stricter requirements. In addition, it introduces a registry for high-risk AI systems and a ban on systems posing unacceptable risks. The EU AI Act will, among others, apply to providers of AI systems, deployers (users) of AI systems, importers and distributors of AI systems and product manufacturers placing on the market or putting into service an AI system together with their own product under their own name or trademark.

As regards automated investment advice, at the moment there is no specific regulation on that. However, as of 1 July 2024, certain requirements will apply to the provision of automated advice. These requirements aim to safeguard the adequate provision of automated advice. Financial service providers that provide automated advice on financial products should:

- designate one or more individuals who are responsible for the automated system and automated advice. These individuals should have the required knowledge and competencies to advise on the relevant financial product themselves;
- conduct an analysis of the automated system before it is used to ensure that it works and all components of the advice are suitable for the client and periodically assess whether the provided automated advice is indeed suitable; and

- take certain measures in case the provided automated advice does not comply with the applicable rules and regulations. These measures include (temporarily) ceasing the provision of automated advice, checking the system to identify the error that has caused the non-compliance and inform the clients that have been affected by such error.

In addition, the AFM has issued guidelines regarding the duty of care of asset managers who offer semi-automatic portfolio management (and investment advice). These guidelines are not legally binding but they bring clarity for asset managers. The guidelines are aligned with Dutch law, Directive 2014/65/EU (Markets in Financial Instruments Directive II) and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

The AFM has also published its views on robo-advice more generally, stating that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider.

Law stated - 1 June 2024

CHANGE OF CONTROL

Notification and consent

Describe any rules relating to notification or consent requirements if a regulated business changes control.

If a qualifying holding (at least 10 per cent of the shares or voting rights, or both) is obtained in certain Dutch financial firms (such as settlement institutions, banks, managers of undertakings for collective investment in transferable securities, investment firms, entities for risk acceptance, premium pension institutions, insurers, reinsurers, payment service providers and electronic money institutions), prior approval by the Dutch Central Bank (DNB) is required. In specific cases, increases in qualifying holdings above certain thresholds are also notifiable to or subject to approval from the DNB.

This also applies to any qualifying holdings in Dutch registered crypto service providers and will apply to cryptoasset service providers authorised under MiCAR.

Law stated - 1 June 2024

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

There is no general framework under which fintech companies are required to have in place procedures to combat bribery or money laundering. Nevertheless, financial firms are generally subject to anti-money laundering and combating the financing of terrorism requirements.

Further, as of 21 May 2020, certain crypto service providers fall within scope of the Money Laundering and Terrorist Financing (Prevention) Act.

This concerns companies, legal entities or natural persons that provide:

- services for the exchange between virtual and fiat currencies; and
- services offering custodian wallets (namely, services to safeguard private cryptographic keys on behalf of customers; consequently, 'soft wallets' do not fall within the scope).

These crypto service providers are required to register with the Dutch Central Bank (DNB), to the extent they provide exchange services between virtual and fiat currency or custodian wallet services 'in or from the Netherlands'. A crypto service provider is providing services 'in the Netherlands' if it has directed its activities to the Dutch market (eg, marketing, use of the Dutch language, offering the possibility to pay via Dutch-specific payment methods (such as iDEAL), availability of the app in the Dutch Google Play Store or Apple App Store, etc). Non-EEA crypto service providers are currently not eligible for registration with the DNB.

Requirements for such registration include (but are not limited to) having in place an adequate integrity policy to ensure ethical operation management. In this policy, an analysis of integrity risks, compliance with the Dutch Sanctions Act, transaction monitoring, reporting of unusual transactions to the Financial Intelligence Unit-Netherlands and customer due diligence must be covered. Further, the DNB applies a 'wallet verification requirement' in relation to incoming and outgoing transactions in the context of sanctions screening.

Other requirements for registration include, among others, that:

- the policymakers of crypto service providers are trustworthy and suitable; and
- the (directors of) holders of a qualifying holding in (at least 10 per cent of the shares or voting rights, or both) and ultimate beneficial owners of crypto-service providers are trustworthy.

Law stated - 1 June 2024

Guidance

Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no regulatory or industry anti-financial crime guidance specifically for fintech companies. However, the Dutch Authority for the Financial Markets, the DNB and the Dutch Authority for Consumers and Markets have set up the InnovationHub to support market operators, such as fintech companies. The purpose of the InnovationHub is to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services.

Furthermore, the DNB has published a brochure titled 'Good practices fighting corruption', and the DNB website provides answers to questions regarding the DNB's integrity supervision of crypto service providers. As regards anti-money laundering and combating the financing of terrorism, the DNB issued Q&As and Good Practices on the Dutch Money

Laundering and Terrorist Financing (Prevention Act) on 8 May 2024 (replacing the DNB's previous guidelines on this). Also, the DNB separately published a chapter from its previous guidelines on the Dutch Sanctions Act. These Q&As and Good Practices and Guidelines are, among others, relevant for payment service providers, e-money institutions and certain crypto service providers.

Law stated - 1 June 2024

DATA PROTECTION AND CYBERSECURITY

Data protection

What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

In the Netherlands, the processing and transfer of personal data is subject to the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the Dutch law implementing the GDPR (the Dutch Implementing Act).

On 25 May 2018, the GDPR came into force with direct effect across the European Union. It governs the collection, storage, recording, viewing, use, adaptation, dissemination and other processing of personal data by businesses, including fintech companies.

The Dutch Implementing Act entered into force on the same date as the GDPR. It sets up the national Data Protection Authority in the Netherlands, and contains certain deviations from the GDPR (as are permitted under the GDPR), mainly in relation to the processing of certain special categories of personal data as mentioned in article 9 GDPR (eg, personal data revealing racial, ethnic origin or political opinions, and genetic or biometric data) and personal data relating to criminal convictions and offences as considered in article 10 GDPR.

There are a limited number of specific data protection-related obligations for providers of payment services under PSD2 that have been implemented in the Decree on Prudential Rules pursuant to the Dutch Financial Supervision Act (FSA). These include:

- the obligation to implement a security policy to protect payment service users from illegal use of their personal data (article 26c of the Decree on Prudential Rules);
- the requirement that access by a payment service provider (not including account information service providers) to personal data is subject to a data subject's explicit consent, and can only be processed and stored insofar as necessary to provide payment services (article 26e of the Decree on Prudential Rules); and
- the requirements that an account information service provider may only access, process and store personal data of data subjects for the purpose of providing the expressly requested account information service and in accordance with the GDPR (article 26j(6) of the Decree on Prudential Rules).

The European Data Protection Board, which has been established by the GDPR, has issued Guidelines on the interplay between the data protection requirements under PSD2 and the GDPR.

Scope

The GDPR applies to the processing of personal data by automated means and, if the data is part of a filing system, non-automated means. Personal data is any information that relates to an identified or identifiable natural person (a data subject). Where personal data is rendered anonymous, it is no longer considered personal data and the GDPR does not apply (noting that the process of rendering personal data anonymous is as such subject to the GDPR as a processing activity). The European Data Protection Board, which is established by the GDPR and consists of the heads of the national supervisory authorities of EU member states and the European Data Protection Supervisor, has issued guidance on anonymisation techniques and the requirements to render personal data truly anonymous.

The GDPR distinguishes between controllers and processors. The controller is the party determining the purposes and means of the processing of personal data, and ultimately accountable for compliance with the requirements of the GDPR. A processor is a party performing the processing of personal data on behalf of a controller (eg, a cloud provider who stores personal data for a fintech company). The processing by a processor is required to be governed by a contract with the controller (a data processing agreement) that addresses certain prescribed requirements and is subject to other specific obligations – also addressed to the processor directly – under article 28 GDPR.

The GDPR has an extra-territorial effect (article 3) in that it not only applies to the processing of personal data by controllers or processors established in the European Union, but also to controllers or processors established outside the EU insofar as they process personal data of data subjects in the EU in relation to (1) the offering of goods or services to such data subjects or (2) the monitoring of their behaviour within the EU.

Processing principles

The GDPR requires that businesses may only process personal data in accordance with certain principles, as further described inaArticle 5 GDPR, including:

- the lawfulness, fairness and transparency principle: personal data must be processed lawfully, fairly and in a transparent manner;
- the purpose limitation principle: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- the data minimisation principle: the personal data processed is to be adequate, relevant and limited to what is necessary for the processing purposes;
- the accuracy principle: personal data processed must be accurate and, where necessary, kept up to date;
- the storage limitation principle: personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the processing purposes; and
- the integrity and confidentiality principle: personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR requires that any processing of personal data must be done pursuant to one of six lawful bases for processing, as set out in article 6 GDPR. The most commonly used lawful bases for processing of personal data are:

- the consent of the data subject to that processing for one or more specific purposes;
- the performance of a contract to which the data subject is a party;
- compliance with a legal obligation to which the controller is subject; and
- the legitimate interests pursued by the controller or a third party insofar as such interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

To have obtained valid consent (the first-mentioned legal basis), consent must be freely given (which is tricky to establish where the data subject and controller are in an employment relationship), specific, informed, unambiguous and capable of being withdrawn as easily as it is given. Also, it must be made by way of a statement or clear affirmative action. This places a significant burden on businesses to ensure that their customers are fully informed on what their personal data is being used for and that their consent can be evidenced.

Data subject rights

The GDPR contains in Chapter 3 a list of rights of data subjects in relation to the processing of their personal data, which include (by way of example) the right to:

- receive certain information about the controller, the purposes and period of the processing, the personal data processed, the legal basis for such processing, the parties receiving the personal data (the processors involved) and whether data will be transferred to third countries, all in a transparent, intelligible and easily accessible manner;
- obtain from a controller the rectification of inaccurate or incomplete personal data;
- obtain the erasure of personal data under certain conditions (right to be forgotten);
- object to processing of personal data and obtain a restriction of processing in certain conditions;
- receive the personal data provided to a controller for portability purposes; and
- not be subject to automated individual decision-making, including profiling.

International transfer of personal data

While the transfer of personal data within the European Economic Area (EEA) is generally permitted under the GDPR, the transfer of personal data by a controller or processor to countries outside the EEA (or to international organisations as defined under the GDPR) is only permitted mainly if:

- the country in question has been deemed by the European Commission in an adequacy decision to ensure an adequate level of personal data protection (article 45 GDPR);

- the controller or processor has provided other appropriate safeguards and enforceable rights and effective legal remedies are available to the data subjects concerned (article 46 GDPR); or
- certain specific derogations apply as set out in the GDPR (article 49).

There are currently 16 adequacy decisions in place, including for Japan, Switzerland, the United Kingdom and the United States (for commercial organisations certified under the EU–US Data Privacy Framework).

Where no adequacy decision exists, commonly used safeguards (which do not require any specific authorisation from data protection authorities) include: (1) the use of standard data protection clauses approved by the European Commission; and (2) binding corporate rules (a set of rules governing intra-group transfer of personal data) approved by competent national supervisory authorities.

In the absence of an adequacy decision or appropriate safeguards, a transfer of personal data to a third country can take place only on one of the following conditions (as stated in article 49 of the GDPR):

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and
- the transfer is made from a register, which according to EU or EU member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or EU member state law for consultation are fulfilled in the particular case.

With regard to the option of obtaining the data subject's consent for a transfer of personal data to a third country, it should be noted that the data subject's explicit (ie, not implied) consent for a particular transfer must be obtained (no blanket consent for repetitive or possible future transfers), and that a request for consent must be expressly and transparently made (not buried in terms and conditions or a privacy notice).

If none of the derogations above are applicable, a final derogation under article 49 GDPR allows for the transfer of personal data to third countries if necessary for the purposes

of compelling legitimate interests pursued by the controller, which are not overridden by the interests or rights and freedoms of the data subject, provided that the transfer is not repetitive, concerns only a limited number of data subjects and the controller has provided suitable safeguards for the protection of the personal data concerned after conducting a risk assessment and has informed both the national supervisory authority as well as the data subjects about the transfer and the compelling reasons pursued.

Other main obligations

The GDPR further includes mandatory requirements to notify national supervisory authorities and (under certain conditions) data subjects of personal data breaches (article 33), the obligation for controllers and processors to keep detailed records on processing (article 30), the obligation for controllers to carry out data protection impact assessments where types of processing are likely to result in a high risk to the rights and freedoms of natural persons (article 35) and requirements for controllers and processors to appoint a data protection officer if they undertake regular and systemic monitoring of data subjects on a large scale, or their core activities consist of processing on a large scale special categories of personal data or personal data related to criminal convictions and offences (article 37).

Remedies, liability and penalties

The GDPR frames rights of data subjects and corresponding obligations for member states to ensure effective judicial remedies for infringements of the GDPR (articles 77–81).

Persons that have suffered material or non-material damages as a result of infringements of the GDPR are entitled to receive compensation from the controller or processor, in the context of which controllers are liable for all damages caused by their processing (including as conducted by processors on their behalf) and processors are liable for the damages caused by their specific processing activities (article 82).

Businesses that infringe the GDPR may, depending on the infringement involved and further circumstances of the infringement, be subject to administrative fines up to €20 million or 4 per cent of global turnover, whichever is higher.

Law stated - 1 June 2024

Cybersecurity
What cybersecurity regulations or standards apply to fintech businesses?

Sector-specific cyber security requirements

Various EU directives and regulations comprise cyber security-related requirements for financial entities, including fintech businesses to the extent that they are regulated under such rules. These requirements have to some extent been further explained in guidelines issued by European supervisory authorities for the financial sector, such as the:

- EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04); and

- EBA Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03).

These requirements have, where necessary to implement EU directives (the requirements under EU regulations have a direct effect and need not be implemented in national legislation), been included in the Dutch Financial Supervision Act (FSA) and secondary legislation. These include the following cybersecurity-related requirements under the PSD2, which have been implemented in the Dutch Decree on Prudential Rules pursuant to the FSA:

- the requirement to implement a security policy document, including a detailed risk assessment in relation to the payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data (article 26c of the Decree on Prudential Rules);
- the requirement to implement business continuity arrangements including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans (article 26d of the Decree on Prudential Rules);
- the requirement to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to payment services, including effective incident management procedures and the obligation to provide to the Dutch Central Bank (DNB), at least on an annual basis, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks (article 26f of the Decree on Prudential Rules);
- the obligation to notify the DNB of major operational or security incidents without undue delay (four hours according to the abovementioned EBA Revised Guidelines on major incident reporting under the PSD2), and, where the incident has or may have an impact on the financial interests of payment service users, the obligation to inform payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident (article 26g of the Decree on Prudential Rules); and
- the obligation to implement adequate security measures and authentication procedures to protect the confidentiality and integrity of payment service users' personalised security credentials (article 26h and 27i of the Decree on Prudential Rules).

The DNB has issued a document called 'Good Practice Information Security', which comprises non-binding guidelines on information security for financial entities under the DNB's supervision and which reflect the DNB's expectations as to the implementation of compliant cyber risk management frameworks. Likewise, the AFM has issued a document called 'Principles for Information Security' for financial entities under its supervision.

Regulation (EU) 2022/2554 (the Digital Operational Resilience Act (DORA)) came into force on 1 January 2023. DORA aims to harmonise IT risk management requirements for the financial sector and further strengthen operational digital resilience. DORA imposes requirements on a wide range of financial entities with regard to IT risk management, IT

incidents, periodic digital resilience testing and third-party IT risk management. Additionally, arrangements for sharing information on cyber threats have been developed. As of 17 January 2025, DORA will apply directly to, among others, fintech businesses in the Netherlands to the extent they undertake regulated financial services.

Cross-sector cybersecurity requirements

The Security of Network and Information Systems Act in the Netherlands (WBNI) implements the requirements under the NIS1 Directive (Directive (EU) 2016/1148) concerning measures for a high common level of security of network and information systems across the European Union. The WBNI imposes risk management obligations and incident reporting requirements on entities in various sectors as specified in the NIS1 Directive that provide essential services and have been designated as such by national supervisory authorities. For the financial sector, this may concern credit institutions, operators of trading venues and central counterparties. The NIS1 Directive has been replaced by the NIS2 Directive, which must be implemented by EU member states by 18 October 2024. The Netherlands is in the process of preparing a new Cyber Security Act to implement NIS2 and replace the current WBNI. The proposal for that new Cyber Security Act is expected to be issued towards the end of 2024 and enter into force during 2025. Like under NIS1, NIS2 (and the expected Dutch Cyber Security Act) will comprise risk management and incident notification obligations in respect of network and information systems used by essential and important entities in various sectors, including for the financial sector credit institutions, operators of trading venues and central counterparties.

The GDPR includes provisions relating to the security of processing, such as the requirement for the controller to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures that are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects. The controller and the processor must also implement these measures to ensure a level of security appropriate to the risk, which may include, among other things:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Law stated - 1 June 2024

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The general rule under the DutchFinancial Supervision Act (FSA) is that a financial services provider must organise its operations in such a way as to safeguard controlled and sound business operations (article 3:17 FSA). Where a financial services company seated in the Netherlands outsources a material aspect of its business operations to third parties, it remains responsible for the outsourced activities and must ensure that the third party concerned complies with the rules imposed on the financial services company (article 3:18 FSA). If a financial services company plans on using a third party for activities for which a licence is required, this can only be done where both parties have a licence for these activities.

Additional rules on outsourcing of material elements of business operations have been set forth in the Decree on Prudential Rules that has been issued pursuant to the FSA. These include, without limitation, the rules that:

- such outsourcing must not obstruct adequate supervision by the authorities or diminish the quality of the internal audit function of the company;
- the tasks and activities of senior management (the persons determining day-to-day management) cannot be outsourced;
- outsourcing by financial services companies of critical or important functions (including payment services) must be notified to the Dutch Central Bank (DNB);
- financial services companies must implement a risk management framework in respect of outsourcing;
- outsourcing contracts must address certain elements set forth in the Decree on Prudential Rules.

The DNB has issued various national guidelines on outsourcing by financial services companies and also generally expects adherence to the Guidelines on outsourcing arrangements issued by the European Banking Authority. For customer due diligence process under the Dutch Money Laundering and Terrorist Financing (Prevention) Act, further detailed outsourcing provisions apply.

The Digital Operational Resilience Act (DORA) harmonises and enhances the requirements for financial services companies regarding the risk management framework to be implemented in relation to their outsourcing of IT services, including as regards the contracts entered into with IT third-party service providers both intragroup and externally. The requirements under DORA will become applicable as of 17 January 2025.

Law stated - 1 June 2024

Cloud computing

Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

If a financial institution wants to make use of cloud computing, it must notify the Dutch Central Bank (DNB) of its intention to do so, regardless of the materiality of the outsourced

activities. Before using cloud computing, the financial institution is required to develop a risk analysis, which must be presented to the DNB. Because the DNB qualifies cloud computing as a specific type of outsourcing, the rules on outsourcing apply. In addition, the DNB expects that the guidelines on outsourcing to cloud service providers as set forth in the Guidelines on outsourcing arrangements issued by the European Banking Authority are taken into consideration.

Law stated - 1 June 2024

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory materials) are protected by copyright. Copyright arises automatically as soon as the computer program is created, registration is not required. Copyrighted works are protected until 70 years after the death of the creator.

Databases underlying software programs may also be protected by copyright and, in certain circumstances, by database right. A database right is a stand-alone right that protects databases that have involved a substantial investment in obtaining, verifying or presenting their contents. The right automatically comes into existence upon creation and expires after 15 years.

Software may also be protected as confidential information or as a trade secret by keeping the software code secret. There are no formal (registration) requirements other than that a trade secret holder needs to take reasonable measures to protect its secret and it needs to have commercial value.

Computer programs and schemes, rules or methods of doing business as such are expressly excluded from patentability under the Dutch Patent Act 1995 and the European Patent Convention. However, patent protection for software may be possible if the inventor is able to demonstrate that the software is novel and inventive and makes a technical contribution over and above that provided by the computer program or business method itself. To obtain patent protection, registration is required with the relevant Dutch and European patent offices and the registration requirements must be followed. Patent protection is limited to 20 years starting from the date of filing the application.

Law stated - 1 June 2024

IP developed by employees and contractors

Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyrights and databases created by an employee during the course of his or her employment are automatically owned by the employer unless the parties have agreed otherwise. Patents protecting inventions made by an employee in the course of his or her

normal duties are owned by the employer. Any other patented inventions will be owned by the employee unless agreed otherwise.

Inventions or copyrights created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed. By contrast, database rights are owned by the person who takes the initiative and assumes the risk of investing in obtaining, verifying and presenting the data in question. Depending on the circumstances, this is likely to be the business that has retained the contractor or consultant.

Law stated - 1 June 2024

Joint ownership

Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Where two or more persons jointly own an intellectual property right, any one of them may use and enforce the right, unless otherwise agreed. Each joint owner may assign or charge its share of the intellectual property right without the other owners' consent. Exploitation of the intellectual property right, including the granting of licences and charging or assigning the intellectual property right, can only be done by the joint owners of the intellectual property right.

Law stated - 1 June 2024

Trade secrets

How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

In the Netherlands, trade secrets are protected by the general law of tort (such as breach of the rules of fair competition) and by the Dutch Trade Secrets Act, which entered into force on 23 October 2018 and implements Directive 2016/943/EU (Trade Secrets Directive). The Trade Secrets Act provides more specific rules for the protection of trade secrets. The Trade Secrets Act defines a trade secret as information that:

- is secret, in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps by the holder of the information to keep it secret.

The Trade Secret Act contains measures and remedies to enforce trade secrets. The secret holder can claim an injunction against further use or disclosure of a trade secret. This includes injunctions against infringing goods, which are goods, the design, characteristics, functioning, production process or marketing of which significantly benefit from trade secrets unlawfully acquired, used or disclosed. The Trade Secret Act includes the possibility for the court to grant the winning party a full cost award of all reasonable and equitable legal costs and other costs.

Measures are available in the Netherlands to prevent public disclosure of trade secrets during court procedures. For example, the court may order oral hearings to be conducted 'behind closed doors' and hand down decisions in which confidential information is redacted. The current Trade Secret Act proposal includes a new rule introducing the option for the court to impose a confidentiality club, limiting the access to trade secrets.

Law stated - 1 June 2024

Branding

What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks either in the Benelux alone (as a Benelux trademark) or across the European Union (as an EU trademark). Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright. Design rights and trademarks are obtained by registering the design or trademark with the relevant authority (eg, the Benelux Office for Intellectual Property, World Intellectual Property Organization or European Union Intellectual Property Office).

The Benelux and EU trademark databases can be searched to identify registered trademarks or applications for a trademark with effect in the Netherlands. It is highly advisable for new businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names.

Law stated - 1 June 2024

Remedies for infringement of IP

What remedies are available to individuals or companies whose intellectual property rights have been infringed?

As a preliminary point, on 1 June 2023, the new Unified Patent Court (UPC) commenced. The UPC offers a single, specialised patent jurisdiction for participating EU member states. The UPC has a court of first instance, which is divided into local divisions. The Netherlands will host one of these local divisions. For European patents with unitary effect (unitary patents) or European patents that designate the Netherlands and are not opted out of this new system, it is also possible to litigate these in the Dutch local division of the UPC.

For the sake of completeness, we note that the below is meant as a listing of remedies available in the Dutch national courts for IP infringements (although these remedies are also available within the UPC).

Remedies available in the Dutch national courts include:

- preliminary and final injunctions (preliminary injunctions are available cross-border);
- damages or surrender of profits;
- delivery up or destruction of infringing products;
- orders to disclose certain information that relates to the infringement;

- publication orders; and
- reimbursement of costs, including court fees and costs of (patent) attorneys and experts (cost orders in Dutch intellectual property litigation are based on guidelines that provide fee caps for compensation that can be awarded in different types of proceedings. The highest fee cap is for highly complex patent litigation in the first instance, for which the fee cap is €250,000. In special circumstances, the courts may deviate from the fee caps in the guidelines).

Law stated - 1 June 2024

COMPETITION

Sector-specific issues

Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The Dutch Authority for Consumers and Markets (ACM) continuously monitors compliance with competition law by companies active in all sectors and also including the financial sector. By means of the Financial Sector Monitor, the ACM carries out economic research into the operation of the financial markets and analyses the risks to competition. In previous years, the ACM presented its findings on competition in this respect. Further, the ACM has specific powers regarding payment system providers and interchange fees.

In 2016, the ACM called for public input on how it can help to boost fintech companies' contribution to competition in the financial sector whereby it indicated it would pay special attention:

- to barriers to entry that prevent the fintech sector from reaching its full potential; and
- to risks involved with rapid technological change that may have adverse effects on competition and innovation.

Following this communication, the ACM has so far looked into the following two specific issues:

- whether regulatory costs constitute barriers to entry for fintech companies. The ACM ordered a study from EY that concluded that such regulatory costs do not constitute obstacles for new providers in the financial sector; and
- whether banks are limiting access of fintech companies – front-end providers and end-to-end providers – to bank accounts and thereby hinder competition in the payment market.

The ACM identified a risk of foreclosure of front-end providers. As a result, the ACM announced that it will actively monitor the behaviour of banks and how they deal with requests for access. In addition, the ACM:

- proposed that where possible, in light of Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2) and the European Commission's Regulatory Technical

Standards, further national implementation of EU law regarding access to bank accounts should enable such access;

- indicated that a system of free access could result in the banks refusing access (which implies that the ACM proposes to allow the banks to ask for compensation for the costs related to providing access); and
- proposed that a light version of the banking licence could be created for fintech companies so that they can offer payment accounts.

As regards end-to-end providers, the ACM considered that the risks of foreclosure were limited. Nevertheless, it proposed to cut the red tape – in addition to the above-mentioned light banking licence:

- by defining objective permit criteria that are related to the actual risks posed by end-to-end providers; and
- by making sure that, in the development of instant payments infrastructures in Europe, fintech companies are able to directly participate in the systems and arrangements for clearing and settlement of payments under non-discriminatory and objective condition

In 2020, the ACM – on request of the Ministry of Finance – conducted a market study into the role of Big Tech (Amazon, Ant Group, Apple, Facebook, Google and Tencent) in the Dutch payment market and more specifically on the segments counter payments, online payments and payments between consumers. In this study, the ACM concluded that the presence of Big Tech at the time was limited but that it is growing and that Big Tech primarily offered consumers innovative means of payment (citing the use of smartphones for payment or the recent entry of Apple Pay on the counter payments segment). The ACM expected the presence of Big Tech, as well as the use of such payment methods by consumers, to increase in years to come and noted that these companies choose to offer payment services to reinforce their ecosystems, rather than being driven by the introduction of PSD2.

The ACM identified the following competition risks:

- access restrictions for new innovative players such as Big Tech and fintechs; and
- Big Tech leveraging its dominant market position in neighbouring markets to tip the payment market (through self-preferencing).

The ACM concluded that an amendment of PSD2 may be to ensure that it also applies to Big Tech as gatekeepers to ensure a level playing field for competitors and a free choice for consumers. The ACM in this respect also fully supports the European Commission's Digital Markets Act, which creates various obligations and prohibitions for certain digital services companies (gatekeepers).

In 2021, after having received complaints from dating-app providers, the ACM concluded that Apple abused its dominant position. The ACM determined that if an app provider offers digital content or services within the app for a fee, the app provider is required to agree to additional contractual conditions set by Apple.

These conditions required app providers to use Apple's payment system for the processing of payments and stipulated that app providers are not allowed to refer within their own

apps to payment options outside the app, for example, to alternative payment options that app providers offer on their websites. According to the ACM, this constituted an abuse of a dominant position. The ACM, therefore, ordered Apple to change its conditions and imposed an order subject to periodic penalty payments. After incurring the maximum penalty payment, Apple changed its conditions and now allows different methods of payment in dating apps in the Netherlands. In view of the ACM, Apple now meets the requirements that the ACM sets under EU and Dutch competition rules.

In 2022, the ACM requested the Ministry of Finance to fix a flaw in the national legislation implementing the PSD2. Because of this flaw, the ACM could only take action if a payment institution had been granted a licence by the Dutch Central Bank. The ACM could not handle complaints or reports about banks filed by payment institutions that had been granted licences from other EU regulators. As a result, the ACM was unable to conduct effective oversight over Dutch banks that refuse to offer a bank account to payment institutions, such as fintechs, from other EU countries. To fix this flaw, the national legislation was amended in 2023.

Law stated - 1 June 2024

TAX

Incentives

Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Investing in the fintech sector is encouraged by the Dutch government. Two main tax incentives are available for fintech companies and investors in the Netherlands, being of the innovation box regime and the research and development (R&D) wage tax rebate.

Innovation box regime

Dutch taxpayers may claim a particular tax treatment providing for an effective corporate income tax rate of 9 per cent instead of the statutory rate of 25.8 per cent (2024 rates) on profits realised in respect of certain intangible assets, such as patents, developed by the taxpayer (the innovation box). The regime applies insofar as the total income from the intangible assets to which the regime applies exceeds the total R&D costs for these assets. Further, the Netherlands applies a nexus approach limiting the benefits of the regime if R&D activities are outsourced to related parties. Software can also qualify as an intangible asset.

Wage tax deduction incentive to invest in R&D

- The R&D tax rebate (wage tax deduction (WBSO)) offers compensation for part of a company's R&D wage costs, other costs, and expenditures. In practice, the WBSO provides for a reduction in payroll taxes to be withheld from the salary of employees engaged in R&D in the Netherlands. As a result, the WBSO decreases a company's personnel costs providing a liquidity benefit to the employer.

- The WBSO amounts to 32 per cent of the first €350,000 of R&D wage and other costs and expenses, and 16 per cent of all further R&D costs and expenses. For start-ups, the tax deduction for the first €350,000 spent on R&D is 40 per cent (2024 rates).

Accelerated deprecation for corporate income tax purposes

In addition to the abovementioned innovation box regime and the WBSO, special tax incentives are available in the Netherlands to stimulate sustainable entrepreneurship. An investment rebate is a tax incentive in the form of an additional deduction amounting to a certain percentage of the investment made. Currently, there are several investment rebates available in the Netherlands. These investment rebates are:

- the small-scale investment rebate (KIA);
- the energy investment rebate (EIA); and
- the environmental investment rebate (MIA).

With respect to the EIA, an additional extension is provided for the flexible depreciation of qualifying investments (VAMIL).

The KIA is applicable when a maximum of €387,580 (amount for 2024) is invested in any relevant financial year. The KIA is not limited to sustainable investments but is generally applicable. To encourage investments in efficient energy assets, the EIA amounts to 40 per cent of the investment in 2024. The EIA applies subject to certain conditions. In 2024, the MIA allowance amounts to 45, 36 or 27 per cent of the investment amount.

Other than the above-mentioned investment rebates, the VAMIL does not create an additional deduction in the corporate income tax return, but provides for a temporary difference by allowing accelerated depreciation on assets in one year up to a maximum of 75 per cent. The remaining 25 per cent is depreciated on a straight-line basis.

Tax treatment of stock options

The taxable moment for payroll withholding tax purposes due on stock options on (non-tradable) shares awarded to employees is deferred to the moment the shares become tradable. This deferral upon request was introduced to attract and retain employees and make the Netherlands more competitive for start-ups and scale-ups by providing a (temporary) liquidity benefit. However, at the employee's discretion, taxation can still take place at the moment of exercise of the stock option.

If not opted for deferral, payroll withholding taxes are to be withheld if an employer grants stock options to an employee when the employee exercises or sells the stock option. The taxable base consists of the fair market value of the stock option at that moment. Due to the legislative change, the taxable moment for payroll withholding tax purposes is by default deferred to when the shares become tradable, unless the employee opts for taxation at exercise. In the latter situation, any increases in value after the moment of taxation will not be subject to payroll withholding tax, and any benefits derived, most notably dividends, are not taxable as taxable wages.

Law stated - 1 June 2024

Increased tax burden

Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Minimum Profit Tax Act

The Minimum Profit Tax Act (applicable as of 2024) implements the Pillar 2 Directive. Pillar 2, an initiative by the OECD/G20 Inclusive Framework, introduces a minimum level of taxation for multinationals and large-scale domestic groups with an annual consolidated revenue of at least €750 million. In scope, multinationals and large-scale domestic groups will at all times pay a minimum effective tax rate of 15 per cent on their worldwide profits, whereby their tax base is determined by reference to the enterprise's financial accounts income after certain tax adjustments have been applied.

Under the Minimum Profit Tax Act, a top-up tax should typically be due if the effective tax rate of the enterprise group is lower than the minimum tax rate of 15 per cent. The primary mechanism is first a qualified domestic minimum top-up tax (QDMTT), followed by an income inclusion rule (IIR). Under the QDMTT, the undertaxed group entity can ensure an effective tax rate of 15 per cent by applying a top-up tax on its own profits, whereas under the IIR additional top-up taxes are payable by a parent entity of a group if one or more constituent members of the group have been undertaxed. The IIR is applied if the QDMTT is not. A secondary fall-back will be provided by an undertaxed payment rule (UTPR) in cases where the IIR are not applied. The UTPR will be introduced on 1 January 2025.

Thirty per cent facility for expats capped at WNT standard

Under the 30 per cent facility, certain employees recruited from abroad to work in the Netherlands can receive a maximum of 30 per cent of their wages tax-free. The 30 per cent facility is capped for expats at the WNT standard (the maximum allowed income in the public-service sector). In 2023, this standard was set at an income of €233,000 per annum. Transitional rules may apply as this cap was introduced as per 1 January 2024.

Law stated - 1 June 2024

IMMIGRATION

Sector-specific schemes

What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The following are the most common corporate immigration schemes in the Netherlands (only relevant for non-EU, EEA and Swiss nationals – third-country nationals – since all EU, EEA and Swiss nationals are free to reside and perform any activities in the Netherlands as long as they wish since there is free movement of workers within the European Union, which is expanded to the EEA and Switzerland).

- Knowledge migrant scheme (highly skilled migrant scheme): this has nothing to do with knowledge as such, but everything with the gross monthly salary (exclusive of holiday allowance, normally 8 per cent of the salary) that is consistent with Dutch salary standards and with thresholds for 2024 that vary from €2,801 to €5,331 per month, depending on age or graduation date in the past three years before applying for such a residence permit from a Dutch or top 200 university from a master's degree or PhD (if graduation is from a university in the Netherlands then bachelor level is also allowed). In addition, the offered salary needs to conform with the prevailing market (namely, normal for the job title). These salary thresholds are indexed each year. However, this does not mean that the salary of the employee needs to change every year. In principle, changes need to be made when the validity of a residence permit is extended, the employee changes employer or the employee changes the purpose of the residence permit. In addition to the aforementioned, the formal employer in most cases needs to hold the status of a recognised sponsor for the purpose of regular labour and knowledge migrants. If the employer is not a recognised sponsor, the employer can apply for that or make use of a payroll company that is a recognised sponsor. The formal employer would borrow their recognised sponsorship, in which case the payroll company would be the formal employer and second the employee to the factual employer. The employer is also able to become a recognised sponsor by submitting an application to the Immigration and Naturalisation Service (IND); as a result, the employer will be considered a reliable partner of the IND.
- Intra-corporate transfer scheme (Directive 2014/66/EU (Intra-Corporate Transit Directive)): if the employee is a specialist, manager or trainee and remains on the payroll of his or her employer outside the European Union, and the employee was already employed at that entity outside the European Union within the same group of companies, he or she may be transferred to the Netherlands under the intra-corporate transfer scheme for up to three years for a specialist or a manager and for up to one year for a trainee (after which he or she can return to the country from where he or she was seconded, or the residence permit can be changed into, eg, a residence permit as a knowledge migrant provided that the salary criterion is met and the employer is a recognised sponsor). The validity of a residence permit as an intra-corporate transferee cannot be extended if, with that extension, the maximum duration of one (trainee) or three (specialist or manager) years is exceeded). No salary thresholds are applicable but the salary criterion for knowledge migrants is an indication, albeit that the salary needs to conform with the prevailing market and, of course, complies with the Dutch minimum wage Act. Also, no recognised sponsorship is required, but is nevertheless advisable for a faster procedure. As a recognised sponsor, the application procedure should just take two weeks instead of 90 days. Some form of intra-EU mobility is possible for a long or a short term, which for a short term would not lead to needing another work permit in the other EU country where the employee is temporarily transferred within the same group of companies. This scheme takes precedence over other schemes if the application or situation falls within the scope of the directive. There is also a national intra-corporate transfer

scheme; however, with this Directive and the national knowledge migrant scheme, the national intra-corporate transfer scheme is not used that often as there are more requirements to be met.

- EU Blue Card scheme (Directive 2009/50/EC (Blue Card Directive): the EU version of the Dutch knowledge migrant scheme but with a higher salary threshold, and where specific education requirements apply. Foreign degrees must be rated by Nuffic. The salary threshold in the Netherlands ranges between €4,265 and €5,331 gross per month, exclusive of holiday allowance for 2024. The lower salary level applies if an employee has completed higher education in the past three years. The higher salary level applies in all other situations, regardless of age. This salary threshold is indexed each year. Recognised sponsorship is not required but is nevertheless advisable due to the more rapid application procedure. The EU Blue Card can be issued for a maximum of four years (depending on the duration of the employment agreement but the employment agreement needs to be for at least one year). After this period, it is possible to renew the EU Blue Card, provided the conditions are met. This scheme remains unpopular in the Netherlands due to the much more flexible national knowledge migrant scheme, although it is renewed in 2024 with the lower salary criterion. The Blue Card does have one advantage: if an employee has a Blue Card that is valid for at least 18 months in another EU country, that employee is already allowed to start working in the Netherlands under the condition that within one month of arrival in the Netherlands, a Dutch EU Blue Card is applied for and in some situations, a permanent residence permit can be applied for earlier than five years.
- International trade regulation: a scheme that may come in handy in certain situations where larger and mostly lower-paid groups of third-country nationals have to come to the Netherlands in the framework of a certain project that has been assessed and approved by the Dutch Employee Insurance Agency (UWV). The salary threshold is the Dutch statutory minimum wage, that on 1 July 2024 increased to €13.68 gross per hour, exclusive of an 8 per cent holiday allowance. To qualify for the international trade regulation, there must be a time-defined trajectory of initially a maximum of three years, and there must be a relationship between the company in the Netherlands and abroad. The workers (employees, clients or director-major shareholders) must come to the Netherlands to perform specialist or managerial duties. The work done may not be of a competitive nature (priority labour supply). This is assessed, among other things, on the basis of the nature, duration and value of the trajectory and nature of the work. Once the trajectory has been approved, the workforce only needs to be notified via a form of the UWV, and the workforce can start work immediately. No recognised sponsorship is necessary.
- Short-term knowledge migrant scheme: this has the same salary criteria as the above-mentioned criteria for the knowledge migrant scheme, but varying from €3,909 to €5,331 gross per month exclusive of holiday allowance and the job in the Netherlands must be a specialist, key, scientific or managerial position. A work permit as a short-term knowledge migrant can be applied for by the employer at the UWV, the recognised sponsor, for short-term assignments for a maximum duration of three out of six months, limited by the duration of the Schengen visa or the free-term requirements of a maximum of 90 out of 180 days.
-

The delivery of goods including assembling, repairing, installing, amending and instructing on the use of those goods, which includes software. This is an exemption in Dutch migration law. No work permit is needed for such work if that work is regarded as incidental labour. In this regard, incidental labour means that the work that needs to be done does not take longer than 12 consecutive weeks within 36 weeks. There is no specific salary criterion, but a salary must be consistent with Dutch salaries for similar work. Should the work, however, not fall within the scope of this exemption, there is also a single permit (that combines a work and residence permit) for the assembly and repair of equipment supplied by foreign companies. The personnel costs must, in that case, not be higher than the to-be-delivered goods, the work must not exceed a period of one year and the workers would need to have specific knowledge to finalise the delivery of the goods for the customer to be able to use the goods. In addition, the following activities are also excluded from the obligation for a work permit, (incidental labour): holding business meetings or concluding agreements with companies and institutions for a maximum period of 13 weeks within a 52-week period and receiving training for a maximum of 12 consecutive weeks within a 36-week period. Note that if the person concerned is going to work, a work permit must be applied for at the UWV, such as a work permit for a knowledge migrant short stay (the short-term knowledge migrant scheme).

- Researcher (Directive 2016/801/EU (Students and Researchers Directive): mostly for researchers and scientists working at universities and other research institutions and companies. A specifically recognised sponsorship is necessary for the purpose of educational institutions. The researcher will work as either a paid researcher, an unpaid researcher with a grant or a PhD candidate and complies with the admittance requirements. Other specific requirements are applicable. The researcher must have at least €1,354.08 gross per month exclusive of holiday allowance as income (salary, scholarship or grant, or in his or her bank account) to comply with the sufficient means of subsistence requirement.
- Intra-EU service provision: exempted from the work permit obligation in the Netherlands if intra-EU service provision is performed under articles 56 and 57 of the Treaty on the Functioning of the European Union, meaning that the work of third-country nationals in the Netherlands by a company based in an EU member state is allowed to provide services to companies in the Netherland. Note that this is only allowed if the third-country nationals are also allowed to conduct similar work in the country of residence. A residence permit obligation in the Netherlands applies after 90 out of 180 days for the third-country national. Based on the third-country national's residence permit issued by the authorisation of another EU member state, this person can stay for 90 out of 180 days in the Netherlands. At day 91, a Dutch residence permit as a cross-border service provider is required. This residence permit at this moment has a maximum duration of two years. This is specifically for third-country nationals living and working legally in EU member state A who temporarily perform services or work for their employer in member state B. No salary threshold applies and no recognised sponsorship is needed. Alongside this, as of 1 March 2020, all cross-border service providers need to notify all their employees (including EU, EEA and Swiss nationals) via www.postedworkers.nl before starting to provide services in the Netherlands. Failure to notify on time will lead to a fine.
-

Several specific training and trainee schemes. These are the most common schemes for corporate migration out of approximately 40 schemes available in the Netherlands, some based on EU law, some purely based on national law. Every case needs to be assessed by an immigration specialist on an individual basis since a different scheme to those stated above might be better suited. Further, there are several short-term work permit exemptions (incidental labour in the Netherlands), for example, for business meetings, receiving training courses or instructions regarding the use of goods manufactured in the Netherlands and services to be provided in the Netherlands. Living legally in the Netherlands is different from working legally in the Netherlands. It is, in principle, forbidden for a third-country national to perform any work in the Netherlands without a work permit, a work permit exemption or a Dutch residence permit with the suitable labour market annotation or single permit, except for very specific exemptions. Sanctions in the case of non-compliance are high – normally an €8,000 fine per illegally working foreigner and per employer in the meaning of the Dutch Foreigners Employment Act – but in most cases of an administrative rather than a criminal nature, additional sanctions may apply including shutting down the business operation in the Netherlands by up to three months.

Since 1 January 2021, UK nationals also need to fulfil the same criteria as any other non-EU, non-EEA citizen or non-Swiss national, as they have become third-country nationals.

Law stated - 1 June 2024

UPDATE AND TRENDS

Current developments
Are there any other current developments or emerging trends to note?

EU developments

Significant current developments relating to fintech seem to be driven at the EU level as a result of EU member states' adoption of the Digital Finance Package in September 2020.

Among other things, the Digital Finance Package introduced the:

- EU Markets in Crypto-Asset Regulation (MiCAR), which entered into force on 29 June 2023. It will apply to certain issuers as of 30 June 2024 and to cryptoasset service providers as of 30 December 2024; and
- Regulation (EU) 2022/2554 (Digital Operational Resilience Act), which will apply as of January 2025.

Further, on 29 May 2024, the European Council approved the Regulation on the use of AI (the EU AI Act). The EU AI Act will enter into force 20 days after publication in the Official Journal of the EU, and its publication is expected to take place in July 2024. In general, the EU AI Act will apply two years after its entry into force, so around mid-2026 (with some exceptions).

In respect of developments relating to anti-money laundering and combating the financing of terrorism (AML/CFT), we note that the EU AML/CFT Regulation and the sixth EU Anti-Money Laundering Directive (AMLD6) were published in the Official Journal of the EU on 19 June

2024. The EU AML/CFT Regulation and AMLD6 will apply as of 27 July 2027 (with some exceptions). Additionally, due to the amended EU Transfer of Funds Regulation, cryptoasset transfer will become subject to its scope as of 30 December 2024.

Another significant development at the EU level is the third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR). On 23 April 2024, the European Parliament adopted PSD3 and PSR, which, among others, introduced further requirements on enhanced strong customer authentication (SCA), access to customers' payments and account information and protection of personal information. PSD3 and PSR will apply to all payment service providers.

Additionally, on 1 June 2023, the Unified Patent Court (UPC) commenced. The UPC is the most significant change in European patent law in 50 years. It offers a single, specialised patent jurisdiction for participating EU member states. It enables patentees to enforce all designations of a European patent in one single enforcement action at the UPC.

With the UPC, patentees also have the option of applying for unitary patents, which will have effect across all participating EU member states. To date, 18 EU member states have ratified the necessary legislation, and 24 are currently signatory states. Signatory states that have not ratified yet can do so at any time. The unitary patent may provide significant cost advantages and a significant reduction of administrative burdens for patentees that normally validate their patents in multiple EU countries.

Finally, in 2022, both the Digital Services Act (DSA) and the Digital Markets Act (DMA) entered into force, which are also relevant for fintech companies. The DSA imposes multiple obligations (most notably transparency and terms of service requirements) on online service providers, including platforms, whereas the DMA creates various obligations and prohibitions for certain digital services companies (gatekeepers). It is unlikely that a fintech company will be designated as a company falling under the DMA or DSA. However, fintech companies, as beneficiaries of these acts, can enforce compliance with obligations by their service providers, such as access to data.

Law stated - 1 June 2024