

# *Danske Bank A/S's privacy notice, for Large Corporates & Institutions, Irish Branch*

Effective from 16 December 2024



## 1. Our role as data controller and the reason for this privacy notice

This privacy notice applies to the processing of personal data of individuals connected to or related to a Large Corporates & Institutions (LC&I) corporate customer of Danske Bank A/S, Irish Branch e.g. an authorised signatory, a beneficial owner, a director, an employee, a corporate card holder, a District user, a guarantor, or another third party. In any of these relationships, Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark, (CVR 61126228) (Danske Bank) processes your personal data as data controller.

Danske Bank has appointed a data protection officer (DPO), whose contact details are as follows:

DPO of Danske Bank A/S, Bernstorffsgade 40, DK-1577 Copenhagen V, Denmark Email address - [dpofunction@danskebank.dk](mailto:dpofunction@danskebank.dk)

And at Irish Branch Large Corporates & Institutions level, a data protection information contact, whose contact details are as follows:

Data Protection Information Contact at Danske Bank A/S, Irish Branch: 7th Floor, The Shipping Office, 20-26 Sir John Rogerson's Quay, Dublin 2, D02 Y049.

This privacy notice sets out how and why and on what legal basis Danske Bank processes your personal data and how we protect your privacy rights.

See section 1.1 for more information on how to contact Danske Bank, in case you have questions related to how Danske Bank processes your personal data.

Please note that we have separate privacy notices applicable to private customers, board members, closely related persons and shareholders, and it may be that these could be relevant to you, depending on your interaction with Danske Bank.



## 2. Types of personal data we collect and process

Depending on your relationship with our LC&I customers and Danske Bank, we process various types of personal data, including, but not limited to, the personal data listed below:

- Identification information, such as your name, PPS number and proof of identity, such as a copy of your passport, driver's licence and/or birth certificate.
- Contact information, including your address, telephone number and email address.
- Educational information, such as your education, profession, work knowledge and experience.
- Information about the services and products we provide to you or our LC&I customer, including information about accounts, cards and access rights.
- Information on how you use our services and products and your preferences in relation to these.
- Information related to your use of our websites, platforms and digital applications, including - to the extent applicable and necessary - traffic, location, tracking and communication data, e.g. collected by use of cookies and similar technology, cf. also Danske Bank's cookie policy.
- Information about the devices you use to access our websites as well as technical information, including the type of device and operative systems.
- Information provided by you about your preferences or your attendance at customer events.
- Tracking data if you have consented to this in connection with signing up for receiving newsletters.
- Information about your visits to our offices, including video surveillance and CCTV footage.
- Recordings of telephone conversations we have with you and of online meetings with you.
- Other personal data we require to use to provide our LC&I customer with specific products or services, or if we are required by law to do so.

Our ability to offer the best possible advice and solutions for you and our LC&I customer very much depends on how well we know you and know our customer. Consequently, it is important that the information you provide is correct and accurate and that you inform us of any changes.



### 3. Why & on which legal basis we process your personal information

Generally, we process personal information about you to provide you or our LC&I customer with the services and products chosen, to offer you or our LC&I customer the best advice and solutions, to protect our LC&I customer, you and Danske Bank against fraud, to fulfil our agreements with you or our corporate customer and to comply with applicable regulations, including data security and data protection requirements.

Below, we list some examples of why and on which legal basis we process your personal data in various contexts:

- When we onboard you as a user of an online product or platform for our LC&I customer, we process your personal data for identification, verification and anti- money laundering purposes. The legal basis for this processing is to comply with a legal obligation\*, cf. GDPR art. 6.1(c), for example, pursuant to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010
- When we provide our LC&I customer with a financial product you have requested on behalf of its behalf, or are considering obtaining on behalf of such customer (such as payment services, accounts, card services, loans, credit facilities, and digital banking solutions, (in some cases by other companies in the Danske Bank Group), customer services, customer relationship management, including registration in our CRM systems, administration, credit assessment, recovery of outstanding debt, handling of complaints and/or making information available to service providers authorised to request information about you or our LC&I customer), we do this to pursue legitimate interests, cf. GDPR art. 6.1(f) [Ireland: GDPR art. 6.1(b) cannot be the legal basis where the contract is with a company, as is always the case for Ireland. Our advice is that the contract has to be with the data subject for that legal basis to apply]
- Sometimes we share your personal data with another company within the Group or transfer your personal data to a third party so that you may receive a quotation for a product or a service, because we have agreed to do so with our LC&I customer and in relation to the transfer of your personal data we pursue legitimate interests, cf. GDPR art. 6.1(f),
- When we communicate with you about the products and services you have requested on behalf of our corporate LC&I customer or send you information on system updates, we do so subject to a legal obligation\*, cf. GDPR art. 6.1(c), or to pursue a legitimate interest, cf. GDPR art. 6.1(f) [Ireland: we cannot use performance of a contract as the legal basis - we have no contracts with data subjects]
- When we improve, develop and manage our IT systems, we may, if necessary, use your personal data to improve or develop products and services and test our systems or to develop, train and test IT and other models. This may be done on the legal basis we have for processing your personal data in our IT systems at the first stage of processing (which could be any of the legal bases mentioned in this section), and/or to ensure a sufficient level of security, cf. GDPR art. 6.1(c), cf. GDPR art. 32, or to pursue a legitimate interest in doing so, cf. GDPR, art. 6.1(f)
- When we set fees and prices for our products and services, including using data analytics and statistics for such purpose, we do this to fulfil contractual purposes, cf. GDPR art. 6.1(b), to pursue a legitimate interest c. GDPR art. 6.1(f) so that you on behalf of our LC&I customer may receive a price quotation or a product offering, and in relation to processing your personal data, we pursue a legitimate interest, cf. GDPR, art. 6.1(f)
- When we carry out fraud detection on card and account transactions, including processing of behavioural data to detect and prevent fraudulent activity in our accounts by identifying unusual, atypical, or suspicious use, registration of payment cards on relevant lists of blocked cards, detection and prevention of fraud, credit fraud and other types of financial crimes, we do so to comply with legal obligations\*, cf. GDPR art. 6.1(c), and to pursue legitimate interests, cf. GDPR art. 6.1(f)
- When we pursue statistical, scientific and/or research purposes as part of research projects or similar, including anonymisation of personal data for such purposes, we pursue legitimate interests, cf. GDPR art. 6.1(f) or we act in the public interest of, cf. GDPR art. 6.1(e)

- We use cookies and similar technology on our website and in our apps for functional, statistical and marketing purposes via digital channels and social media platforms if you have consented to this, cf. the cookie requirements for collection of data and GDPR, art. 6.1(a) for the subsequent use of data. We refer to our cookie policy for further information (Danske Bank's cookie policy)
- When we assess, check, test and monitor our compliance with internal company policies and rules, regulatory and legislative requirements, e.g. in relation to data protection, financial crime or market integrity, we process your personal data subject to legal obligations\*, cf. GDPR art. 6.1(c) and to pursue legitimate interests of Danske Bank, cf. GDPR art. 6.1(f)
- We process your personal data for security reasons, for instance for various logging purposes, cf. GDPR art. 6.1(c) and art. 32 and GDPR art. 6.1(f).
- We use video surveillance and record the front of buildings, entrances to our branches and other premises, reception and customer areas, ATMs, and counters where we are pursuing legitimate interests, cf. GDPR art. 6.1(f)
- When we collect, share and use personal data to build, maintain and use models for credit risk exposure and Internal Ratings Based (IRB) modelling to assess capital requirements, we do so with reference to the Capital Requirement Regulation (CRR) which is required as part of Danske Bank's risk management, cf. GDPR art. 6.1(c)
- When we send you newsletters, we process your personal data, and we use your email and name for documentation purposes to send you articles, news and updates because you have requested this service from us, cf. GDPR art. 6.1(f). We may also invite you to events and send you marketing material in areas that we think may have your interest, and we track which articles have your interest and which you open based on your consent, cf. GDPR art. 6.1(a)
- When we check, test and monitor our compliance with regulatory and legislative requirements e.g. in relation to MIFID and MAR, data protection, financial crime and/or market integrity. If you are participating in a Teams meeting with a Danske Bank employee who is recorded for MIFID/MAR purposes the meeting may likewise be subject to monitoring. cf. GDPR art 6.1(c) and GDPR art 6.1(f).
- We also carry out several other legal, regulatory, administrative and compliance-related processing activities which entail processing of personal data, including identification and verification according to anti-money laundering legislation and risk management, cf. GDPR art. 6.1(c), and to pursue legitimate interests of Danske Bank, cf. GDPR art. 6.1(f)

\*When we refer to processing of your personal data due to 'legal obligations', this refers to legal requirements under any of the following laws (please note that this list is not exhaustive):

- Criminal Justice (Money Laundering and Terrorist Financing) Act 2010
- Taxes Consolidation Act, 1997
- Credit Reporting Act 2013
- European Union (Markets in Financial Instruments) Regulations 2017
- Consumer Protection Code 2012
- FATCA/CRS
- The General Data Protection Regulation
- The EU Regulation on markets in financial instruments (MiFIR)
- The EU Regulation on market abuse (the Market Abuse Regulation)

\*Or any amendment or replacement of this law which may arise, or to comply with:

- Court orders arising in civil or criminal court proceedings
- Binding requests from regulatory bodies such as the Central Bank of Ireland
- Binding search warrants, productions orders and other orders requiring the bank to provide assistance in civil or criminal matters



## 4. Sensitive personal data

Some of the information we process about you may be sensitive personal data (also known as special categories of data). Sensitive personal data or special categories of data are subject to specific processing conditions, and we try to avoid processing such personal data when possible. However, in some instances we need to process sensitive personal data about you.

Below you can see examples of types of sensitive personal data we process about you, why we do it and our legal basis (exceptions in GDPR art. 9) for doing so.

- We process sensitive personal data about you when you provide us with information about your food preferences, which may include information about allergies, e.g. if you participate in hospitality events that we arrange with your consent, cf. GDPR, art. 6.1(a) and 9.2(a)
- We may process sensitive personal data about you to comply with legal requirements that apply to us as a financial institution in other legislation, such as screening and identification and verification cf. GDPR art. 6.1(c), 9.1(g) and 9.3
- We may process sensitive personal data about you if such processing is necessary for the establishment, exercise or defence of legal claims, cf. GDPR art. 9.1(f)



## 5. How we collect the personal data we have about you

### *Personal data collected from you*

We collect information that you share with us or that we obtain by observing your actions, including for example when:

- You fill in applications and other forms for ordering services and products
- You submit specific documents to us
- You participate in meetings with us on behalf of our LC&I customer/your employer
- You talk to us on the phone
- You use our website, mobile applications, products, and services
- You participate in LC&I customer surveys organised by us
- You communicate with us by letter and digital means, including emails, or on social media
- You use our digital solutions and apps or visit our websites
- We collect personal data from electronic communications, telephone and video recordings and monitoring
- You participate in hospitality events organised or hosted by us
- We track your subscription to newsletters

We monitor and store electronic communications and record, monitor and store incoming and outgoing calls you have with relevant employees, for instance when we chat, email or speak on the phone with you, according to the EU (Markets in Financial Instruments) Regulations (MiFID I and II). We also store video/CCTV recordings of you if you have visited our premises, because it is in our legitimate interests to do so to protect the security of our branch.

### *Personal data collected from use of cookies*

We may use cookies and similar technology on our websites and in our digital solutions and apps. When you first enter one of our websites or download our apps, we set necessary cookies to enable you to use our services. If you consent to additional cookies, such as functional, statistical and/or marketing cookies, we set cookies according to your consent in order to measure, analyse and improve the use and performance of our products and services and to the extent applicable and relevant to tailor and send you relevant marketing messages.

Some of the marketing cookies are owned by third parties, such as Meta or Google. We share responsibility (joint controllership) for such third parties' use of your personal data which is collected by way of cookies and processed for our benefit. We refer to our cookie policy ([Danske Bank's cookie policy](#)) for further information.

## *Personal data we collect from third parties*

We receive and collect data from third parties, including for example from:

- The corporate customer of Danske Bank by which you are employed/to which you are related
- Shops, banks, payment and service providers when you use your corporate credit card or debit card or other payment services.
- We process the personal data to execute payments and prepare account statements, payment summaries and the like
- The Central Office of the High Court, the Companies Registration Office as well as other publicly accessible sources and registers. We process the data for identification and verification purposes and to update data and check personal data accuracy, cf. GDPR art. 6.1 (f),
- Credit rating agencies and warning registers. We collect and process the personal data to perform credit assessments. We update the personal data regularly
- Other entities of the Danske Bank Group, for example in order to provide you with better customised products and services
- Other entities of the Danske Bank Group, if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management control and/or reporting requirements established by law such as the Capital Requirement Regulation (CRR)
- External data controllers, such as business partners (including correspondent banks and other banks) and vendors, if we have your consent or if permitted under existing legislation, for example in order to provide you or our business customer with a service or product provided by an external business partner you have signed up for, to enable our customers to use banking services abroad or to prevent and detect money laundering, fraud, abuse and loss
- The Central Credit Register in accordance with our obligations under the Credit Reporting Act 2013.



## *6. Third parties that we share your personal data with*

We will keep your information confidential under applicable banking confidentiality rules. However, where we have due cause we may disclose and share relevant personal data with group companies and third parties, who are also obliged to keep your personal data confidential. Some examples are listed below:

- Other entities in the Danske Bank Group in order to provide you with all aspects of the product or service we are providing to the corporate customer with which you are connected, or to seek approval to do so e.g. in order to obtain credit approval for a loan, and if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management, control and/or reporting requirements.
- Other entities of the Danske Bank Group, if existing legislation allows or requires us to share the information, for example if it is necessary to comply with group-based management or risk management requirements imposed by law or regulations (e.g., Capital Requirement Regulation) and/or reporting requirements established by law or required by regulators
- If you have asked us to transfer money to others on behalf of the LC&I customer, we disclose such personal data about you as is necessary to identify you and to perform the transaction
- When we process international payments, your personal data may be processed by Swift in the context of Swift's Transaction Processing Services, which enable us to send and receive financial messages or files, and to pre-validate, track and manage financial transactions. For further information on the data protection practices of Swift in relation to the processing of your personal data in the context of Swift's Transaction Processing Services, please consult Swift's Personal Data Protection Policy (PDPP), cf. Data Protection Policies | Swift

- Service providers authorised as an account information service, payment initiation service or card-based payment instrument provider, if you (or someone who via our online services can view information about the LC&I Customer's accounts or initiate payments on its behalf) request such a service provider to receive information about you.
- Corporate card producers, when cards are imprinted with your personal data
- Card issuers, payees and holders of lists of blocked cards, e.g., Nets, in case you request us to block your corporate debit or credit card, or if we have reasonable suspicion of card abuse or for Nets to be able to prevent fraud
- Guarantors, individuals holding a power of attorney, lawyers, accountants, or others you on behalf of our LC&I customer have authorised us to share information with
- If the LC&I customer by whom you are employed/with whom you are associated has joint financial products with someone we may be required to share your information, with your co-product holder/owner
- Nets and other banks, if required or permitted under existing legislation, to prevent and detect money laundering, fraud, card abuse and loss
- Lawyers, accountants or consultants related to the Danske Bank Group
- Courier services e.g. when delivering a corporate credit card to you/the LC&I customer by whom you are employed
- IT service and outsourcing providers as well as personal data processors to provide services to us and our corporate customers
- Social media companies, such as Meta and Google, when you have given your consent for direct marketing purposes
- Public authorities and regulatory bodies as required by law or upon their request, including to an Garda Síochána and Revenue Commissioners under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (and any replacement or amendment thereof), to the Revenue Commissioners in accordance with the Taxes Consolidation Act 1997 and other tax legislation, to the Central Bank of Ireland to comply with our obligations under the Credit Reporting Act 2013 and other law and for statistical and other purposes, to the courts, to the Data Protection Commission, to the Financial Services and Pensions Ombudsman, to the Credit Review Office, to the Criminal Assets Bureau, to US, EU and other designated authorities in connection with combating financial and other serious crime, and to fraud prevention agencies.
- Third party providers such as platform providers and forensic providers who are assisting us with providing information to a regulatory body or other public authority
- Guarantors, individuals holding a power of attorney, the lawyers advising you or the corporate body with which you are connected, the accountants advising you or the corporate body with which you are connected, and others you have authorised us to share the information with.
- For social and economic research or statistics purposes, including where it would be in the public interest.
- In connection with transactions (including mergers and acquisitions) which entail transfer of all or part of the LC&I customer's business to another company, we may share your personal data to the extent necessary to complete the transfer and the LC&I customer relationship within the framework of the legal requirements we have to comply with.





## 7. Transfer of personal data to third countries

Your personal data may be processed by our business partners within the EU/EEA in connection with our request to provide you the LC&I Customer by whom you are employed with various services on our behalf.

In some cases, we use various IT suppliers, business partners, and consultants, etc., who can access personal data from countries outside the EU/EEA ('third countries'), if necessary, despite such personal data generally not being stored in the third countries. Such IT providers, partners, etc. are subject to data processing or data sharing agreements with us, which ensure that they process personal data only in accordance with the GDPR and applicable EU and national data protection laws.

We primarily choose providers/partners who process personal data within the EU/EEA, and secondly suppliers in countries that appear on the EU Commission's list of safe third countries, and only if necessary suppliers in other third countries.

Accordingly, we rely on different legal bases depending on the country of the personal data recipient

- If we transfer your personal data to parties in countries where the European Commission has found that the country ensures an adequate level of protection, we rely on the adequacy decision of the European Commission as our GDPR art. 45 transfer basis
- If we transfer your personal data to parties located in the USA, we may rely on the EU-US Data Privacy Framework to certified parties as our GDPR art. 45 transfer basis
- If we transfer your personal data to other third countries, we may rely on the European Commission's standard contractual clauses (also known as SCCs) or business partner's binding corporate rules (also known as BCRs) together with implementation of adequate supplementary measures or carry out a review of local legislation to ensure that your personal data receives an essentially equivalent level of protection to that guaranteed in the EU/EEA, if and where deemed necessary as our legal basis for transfer under GDPR art. 46
- We may also transfer your personal data to parties outside the EU/EEA based on the specific exemptions set out in GDPR art. 49, for example in GDPR art. 49.1(e), if the transfer is necessary for our establishment, exercise or defence of a legal claim

When transferring personal data to a business partner outside of the EU/EEA, we ensure that our transfer of your personal data is conducted in accordance with GDPR Chapter V.

You can read more on personal data transfers to third countries

- On the Danish Data Protection Agency's website - <https://www.datatilsynet.dk/english> and
- On the EU Commission's website - [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu\\_en](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en)



## 8. How long do we store your personal data?

We keep your personal data only for as long as it is needed for the specified purposes for which your personal data was registered and used or as required by law for specific purposes stated by the legislator. The personal data will subsequently be deleted or irreversibly anonymised.

We have many different processes where we use your personal data and many different legal bases for retention of your personal data. Our retention criteria and retention periods vary. Below you see some examples of retention periods, but please note that the list is not exhaustive.

- We keep your account information for up to 10 years in accordance with the statutory limitation periods
- We keep your Know Your Customer information for as long as our corporate LC&I customer is a customer, and for an additional seven years



- We keep credit and collateral agreements for up to 10 years after expiry to document our agreement so we may defend our legal rights within statutory limitation periods
- We keep your consent to our use of cookies for one year unless you withdraw it earlier
- In one circumstance, we keep your personal data for a period of up to 30 years. This is exclusively for use in our Internal Ratings Based (IRB) models used for Danske Bank's risk management and calculation of capital requirements under the Capital Requirements Regulation (CRR) and where we are required to include and document financial
- We keep your voice recordings which relate to our markets business for five seven years under MiFID I and II. Reference is made to our recording of phone conversations and their retention in our General Terms and Conditions - Large Corporates & Institutions
- If you have asked for a quotation on a loan or another product or service on behalf of a potential LC&I customer, your personal data will normally be stored for six months, even if no customer relationship is established, but it may for some purposes be stored longer to comply with legal obligations, for example under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

## 9. Your rights

Your rights in relation to personal data are described below. To exercise your rights, you can use any channel to contact us, for example

- Data Protection Officer, Bemstorffsgade 40, 1577 København V, Denmark, e-mail: [dpofunction@danskebank.com](mailto:dpofunction@danskebank.com)

### *Right to access your personal data*

You have the right to request access to your personal data and to request information about the processing we carry out. Your right of access may, however, be restricted by legislation, protection of another person's privacy and consideration for our business and practices. Access to video surveillance may be restricted due to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to employees. Our know-how, business secrets as well as internal assessments and material may also be exempt from the right of access.

If you wish to exercise your right of access under the GDPR, the best way to contact us is for instance to write to [GDPR-insight@danskebank.dk](mailto:GDPR-insight@danskebank.dk). However, you may also contact us via your adviser or via a message in District, Danske eBanking or Danske Mobile Banking.

### *Rights related to automated decision-making*

When we use automated decision-making in our processes, you will always be notified separately in advance about our legal basis for this and your option to not to be subject to the automated decision making. Furthermore, you will be informed about the reasoning behind the automated decision-making, and you will be given the opportunity to express your point of view and to object to the decision, and of your right to request a manual review of any automated decision.

### *Right to object to processing*

In certain circumstances, you have the right to object to the processing of your personal data, for instance when we use automated decision-making processes, or, for example, when the processing is based on our legitimate interests.

You have the right to object to our use of your personal data for direct marketing purposes, including profiling that is related to such purpose.

### *Right to rectification of your data*

If your personal data is inaccurate, you are entitled to have your personal data rectified. If your personal data is incomplete, you are entitled to have the personal data completed, including by means of providing us with a supplementary statement.

## *Right to erasure ('right to be forgotten')*

You are entitled to have your personal data erased if the personal data is no longer necessary for the purposes for which it was collected.

However, in the following cases, we are required to keep your personal data

- To comply with a legal obligation\*, for instance if we are obliged by law to hold your personal data for a certain period, for example according to the Danish Anti-Money Laundering Act or the Danish Bookkeeping Act. In such situations, we cannot erase your personal data until the required retention period has expired
- For the performance of a task carried out in the public interest, such as sending statistical data to the Danish Central Bank (Nationalbanken)
- For establishment, exercise, or defence of legal claims

## *Restriction of use*

If you believe that the data we have registered about you is incorrect, or if you have objected to our use of the personal data, you are entitled to obtain restricted processing of your personal data for storage only until we can verify the correctness of the personal data or if our legitimate interests outweigh your interests or not

## *Withdrawal of a consent*

Where consent is the legal basis for a specific processing activity, you can always withdraw your consent at any time by contacting Danske Bank (see the section above or section 1.1). Please note that if you withdraw your consent, we may not be able to offer you specific services or products. Please also note that we will continue to use your previously collected personal data, for example in order to fulfil an agreement we have made with you or if we are required by law to do so. Some consents are provided for one specific process only (such as consent to sharing personal data with a third party), also called one-time consents. Withdrawal of a one-time consent will not have legal effect due to the nature of the consent.

## *Data portability*

Under specific circumstances, you have the right to receive personal data which you have provided to us yourself in a structured, commonly used and machine-readable format for personal use. You also have the right to request that we transmit this data directly to another data controller



## 10. Changes to this privacy notice

We are required to update this privacy notice on a regular basis. When we do, you will see that the 'effective from' date at the top of this document changes. If changes to how your personal data is processed will have a significant effect on you personally, we will take reasonable steps to notify you of the changes to allow you to exercise your rights (for example to object to the processing).



## 11. Contact details and how to complain

You are always welcome to contact us if you have questions about your privacy rights and how we process personal data. Please contact us at:

Data Protection Officer, Bernstorffsgade 40, 1577 København V, Denmark, e-mail: [dpofunction@danskebank.com](mailto:dpofunction@danskebank.com)

And you can drop a line to our local data protection information contact at:

Data Protection Information Contact at Danske Bank A/S, Irish Branch: 7th Floor, The Shipping Office, 20-26 Sir John Rogerson's Quay, Dublin 2, D02 Y049.

If you are dissatisfied with how we register and use your personal data and your dialogue with the Data Protection Officer has not led to a satisfactory outcome, you can contact our complaints handling unit by writing to the Data Protection Information Contact and the Legal Team (C&I), both at 7th Floor, The Shipping Office, 20-26 Sir John Rogerson's Quay, Dublin 2, D02 Y049.

You can also lodge a complaint with the Data Protection Commission: Canal House, Station Road, Portarlington, R32 AP23 Co. Laois, email: [info@dataprotection.ie](mailto:info@dataprotection.ie) phone: +353 (0)57 868 4800 or +353 (0)761 104 800.

If, for example, your residence or the place of the alleged infringement is in or is related to another member state than Ireland, you can typically also lodge a complaint with the supervisory authority for data protection in that member state. You also always have the option to try your case in court.