Bord na Móna Data Protection Privacy Policy - Schedules

SCHEDULE 1
Definition of key data protection terms

"**Data Controller**" means the entity that controls Personal Data, by deciding why and how such Personal Data is Processed.

"**Data Processor**" means the party that Processes Personal Data on behalf of the Data Controller (for example, a payroll service provider).

"**European Economic Area**" or "**EEA**" means Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK, Iceland, Liechtenstein, and Norway.

"**Personal Data**" is any information relating to a living individual which allows the identification of that individual. Personal Data can include:

- a name,
- an identification number;
- details about an individual's location; or
- any other information that is specific to that individual.

"**Processing**" includes collecting, using, recording, organising, altering, disclosing, destroying or holding Personal Data in any way. Processing can be done either manually or by using automated systems such as information technology systems and "**Process**" and "**Processing**" shall be interpreted accordingly.

"**Profiling**" is the automated Processing of Personal Data for the purpose of assessing certain aspects relating to an individual so as to analyse or predict the individual's performance, decisions or behaviour.

"**Sensitive Personal Data**" are types of Personal Data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special Categories of Personal Data also include the Processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation and any Personal Data relating to criminal convictions or offences.

"Proxy Access" is where a manager is granted access to another user's Outlook mailbox where access is necessary for the proper and uninterrupted functioning of the business.

SCHEDULE 2
Confidentiality Code of Conduct

Bord na Móna employees and all others who work with or on behalf of Bord na Móna must comply with this confidentiality code of conduct (the "**Code**"). *Bord na Móna will ensure that all those subject to this policy are made aware of it at the outset of their work with the company*.

1. What is Confidential Information?

"Confidential Information" means all business, technical, financial, operational, administrative, marketing, economic and other information and material relating to Bord na Móna's business, and all Personal Data of employees or customers of Bord na Móna either in written, oral or any other form, to which you may have access.

2. Confidentiality and Non-Disclosure Requirements

Confidentiality is an intrinsic element to the work of Bord na Móna. The importance of confidentiality must be clearly understood by all Bord na Móna employees and all others who are or will be required to work with or on behalf of Bord na Móna.

2.1 For the duration of employment with Bord na Móna and at all times after the termination of employment with Bord na Móna, employees must keep all Confidential Information secret and treat it as confidential and must not, without the prior written consent of Bord na Móna (which may be given, if at all, on such terms as Bord na Móna considers appropriate), be disclosed (whether in written, oral or in any other form) in whole or in part to any other person. Employees must not use the Confidential Information for any purpose other than in connection with their role as an employee of Bord na Móna.

2.2 Employees cannot discuss any Confidential Information relating to Bord na Móna (or related Companies or their businesses) or data in respect of which Bord na Móna owes an obligation of confidence to any third party during or after their employment except in the proper course of their employment or as required by law.

2.3 Employees cannot remove or copy any document or things belonging to Bord na Móna which contain any Confidential Information from Bord na Móna's premises at any time without proper advance authorisation.

2.4 Employees must return to Bord na Móna upon request and, in any event, upon the termination of their employment, all documents and things belonging to Bord na Móna or which contain or refer to any Confidential Information and which are in your possession or under their control.

3. Maintaining Confidentiality

Bord na Móna and all others who are or will be required to work on behalf of Bord na Móna or with documentation and/or related systems have an obligation to ensure confidentiality and compliance with the Data Protection Law, Bord na Móna's IT security policies, which have been separately notified to employees, and the security measures outlined in the Data Security and Storage Guidelines must be adhered to.

SCHEDULE 3

Third Party Disclosures

Type of third party	Examples
Service providers	External third party service providers, such as security professionals, accountants, auditors, experts, lawyers and other professional advisors; travel assistance providers; call centre service providers; IT systems, support and hosting service providers; advertising, marketing and market research, and data analysis service providers; banks and financial institutions that service our accounts; document and records management providers; and other third party vendors and outsourced service providers that assist us in carrying out business activities.
Government / Judicial authorities	We may also share Personal Data with: (a) government or other public authorities (including, but not limited to, courts, regulatory bodies, law enforcement agencies, tax authorities and criminal investigations agencies); and (b) third party participants in legal proceedings and their accountants, auditors, lawyers, and other advisors and representatives, as we believe to be necessary or appropriate.

SCHEDULE 4
CCTV Policy

Introduction
Closed circuit television systems ("CCTV") are installed in all premises and some other company assets such as company vehicles, (the "Relevant Assets") under the control of Bord na Móna Plc and its subsidiaries (the "Company").

Purpose of Policy
The purpose of this Policy is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of all Relevant Assets operated by the Company in Ireland.

CCTV systems are installed both internally and externally in all Relevant Assets for the purpose of enhancing security of Company premises and associated equipment, as well as creating awareness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of all assets during both the daylight and night hours each day.

CCTV surveillance is intended for the purposes of: protecting Company buildings and assets, both during and after hours; and promoting the health and safety of staff and visitors. In certain circumstances CCTV footage may be used in the context of employee disciplinary proceedings, internal and external investigations into accidents and other incidents and, if necessary, in legal proceedings.

Scope
This Policy applies to all Company personnel and visitors and relates directly to the location and use of CCTV and to the monitoring, recording and subsequent use of material recorded by CCTV.

General principles
The Company has a responsibility to protect its property, equipment and resources as well as to provide a sense of security to its employees and visitors. The Company owes certain duties under the provisions of health and welfare at work legislation and utilises CCTV as an added mode of security.

The use of CCTV will be conducted in a professional, ethical and legal manner.

Use of CCTV is required to be compliant with this Policy following its adoption by the Company. Recognisable images captured by CCTV are subject to the provisions of the General Data Protection Regulation (EU 2016/679) and the Data Protection Act 2018 (the "Data Protection Law") to the extent they are personal data. "Personal Data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller, with the Company being the data controller.

Use of CCTV footage
Information obtained through CCTV may only be released when authorised by the Information Officer.

Any requests for records of CCTV images by An Garda Síochána will be fully recorded and legal advice will be sought if any such request is made, before any images are disclosed (see "Access" section below).

CCTV monitoring of public areas, for security purposes will be conducted in a manner consistent with all existing policies adopted by the Company.

Video monitoring of public areas, for security purposes, within Company premises, is limited to uses that do not violate the reasonable expectation to privacy.

Lawful basis For processing

The use of CCTV is necessary in order to protect the legitimate interests of the Company. Specifically, these legitimate interests include:

- protecting Company staff, buildings and other assets, both during and after hours;
- protecting and promoting the health and safety of staff and visitors (which is also necessary to protect their vital interests);
- ensuring fair outcomes in the context of employee disciplinary proceedings; and
- ensuring that the legitimate interests of the Company are adequately protected in the event of workplace accidents or other incidents.

The Data Protection Law requires that personal data is adequate, relevant and not excessive for the purpose for which it was collected. This means that the Company needs to be able to justify the obtaining and use of personal data by means of CCTV.

For instance, the use of CCTV to control the perimeter of a building for security purposes has been deemed to be justified by the Company. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

Information may be used as part of or in conjunction with an investigation process and all relevant parties will have the opportunity to view and comment on such footage. Examples of the use of CCTV footage for disciplinary purposes include but are not limited to; establishing the facts of an alleged incident where other evidence is in conflict; as evidence for alleged incidents of stock loss, theft or misuse of time and attendance systems; as evidence of health and safety incidents. It will not generally be used for on-going performance management purposes.

Location of cameras

The Company has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas shall be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Notification – signage

A copy of this Policy is available on request to employees and visitors to the Company's premises. This Policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for use of CCTV.

Signage is in place at each location in which CCTV cameras are sited to indicate that CCTV is in operation. Signage shall include the contact details of the data controller.

WARNING
CCTV cameras in operation
For more information contact [phone number]

Storage & retention

The Data Protection Law provides that personal data shall not be kept for longer than is necessary for the purposes for which they were obtained. The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out in this Policy. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Access

Recorded footage and the monitoring equipment must be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to images shall be maintained.

In relevant circumstances, CCTV footage may be disclosed:

- to An Garda Síochána where the Company (or its agents) are required by law to make a report regarding the commission of a suspected crime;
- following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Company property;
- to data subjects (or their legal representatives), pursuant to an access request under the Data Protection Acts where the time, date and location of the recordings is furnished to the Company;
- to individuals (or their legal representatives) subject to a court order or another legal obligation;
- to the Company's insurance company (and their legal advisors) where the insurance company requires same in order to pursue or defend a claim for damage done to the insured property; and/or
- to certain other bodies/agencies where the Company is required to do so or where it is necessary for the Company to do so.

On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted in line with the above retention section, and provided also that an exemption/prohibition under the Data Protection Acts does not apply to the data in question. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the Company. The Company must respond within one month.

A person should provide all the necessary information to assist the Company in locating the recorded CCTV images, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be "personal data" and may not be disclosed by the Company.
In giving a person a copy of their data, the Company may provide a still/series of still pictures or a disk, USB or other data storage device containing relevant images. However, other people's images will be obscured before the data is released.

Responsibilities
The Company will:

- ensure that the use of CCTV is implemented in accordance with this Policy;
- oversee and co-ordinate the use of CCTV within the premises for the purposes set out in this Policy;
- review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy;
- maintain a record of access (e.g. an access log) to or the release of any material recorded or stored in the system;
- ensure that the perimeter of view from fixed location cameras conforms to this Policy both internally and externally;
- maintain a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located on Company premises;
- ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing;
- ensure that recorded CCTV images are stored in a secure place with access by authorised personnel only; and
- ensure that recorded CCTV images are stored for a period not longer than 30 days and will then be erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Information Officer of the Company.

Security companies
Where the CCTV system is controlled by a security company contracted by the Company, the Company will have a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data and what security standards are to be in place regarding the system and the recorded CCTV images.

Implementation & review
The date from which the Policy will apply is 25th May 2018. The Bord na Móna Policy Working Group will monitor the implementation of the Policy. The Policy will be reviewed and evaluated from time to time. Ongoing review and evaluation will take cognisance of changing law or guidelines

(e.g. from the Office of the Data Protection Commissioner, An Garda Síochána, etc.), as well as feedback from staff and others.

If you have any comments or queries on this policy or the Company's implementation of CCTV, please contact informationofficer@bnm.ie.

SCHEDULE 5
Data Subject Rights

Description	When is this right applicable?
Right of access to Personal Data You have the right to receive a copy of the Personal Data we hold about you and information about how we use it.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to rectification of Personal Data You have the right to ask us to correct Personal Data we hold about you where it is incorrect or incomplete.	This right is applicable at all times when we hold your Personal Data (subject to certain exemptions).
Right to erasure of Personal Data This right entitles you to request that your Personal Data be deleted or removed from our systems and records. However, this right only applies in certain circumstances.	Examples of when this right applies to Personal Data we hold include (subject to certain exemptions): when we no longer need the Personal Data for the purpose we collected it; if you withdraw consent to our use of your information and no other legal justification supports our continued use of your information; if you object to the way we use your information and we have no overriding grounds to continue using it; if we have used your Personal Data unlawfully; and if the Personal Data needs to be erased for compliance with law.
Right to restrict processing of Personal Data You have the right to request that we suspend our use of your Personal Data. Where we suspend our use of your Personal Data we will still be permitted to store your Personal Data, but any other use of this information will require your consent, subject to certain exemptions.	You can exercise this right if: you think that the Personal Data we hold about you is not accurate, but this only applies for a period of time that allows us to consider if your Personal Data is in fact inaccurate; the Processing is unlawful and you oppose the erasure of your Personal Data and request the restriction of its use instead;

	we no longer need the Personal Data for the purposes we have used it to date, but the Personal Data is required by you in connection with legal claims; or you have objected to our processing of the Personal Data and we are considering whether our reasons for processing override your objection.
Right to data portability This right allows you to obtain your Personal Data in a format which enables you to transfer that Personal Data to another organisation. You may have the right to have your Personal Data transferred by us directly to the other organisation, if this is technically feasible.	This right will only apply: to Personal Data you provided to us; where we have justified our use of your Personal Data based on: o your consent; or o the fulfilment by us of a contract with you; and if our use of your Personal Data is by electronic means.
Right to object to processing of Personal Data You have the right to object to our use of your Personal Data in certain circumstances. However, we may continue to use your Personal Data, despite your objection, where there are compelling legitimate grounds to do so or we need to use your Personal Data in connection with any legal claims.	
Rights relating to automated decision making and Profiling You have the right not to be subject to a decision which is based solely on automated processing (without human involvement) where that decision produces a legal effect or otherwise significantly affects you. This right means you can request that we involve one of our employees or representatives in the decision making process.	This right is not applicable if: we need to make the automated decision in order to enter into or fulfil a contract with you; we are authorised by law to take the automated decision; or the decision is based on your explicit consent.
Right to withdraw consent to processing of Personal Data Where we have relied upon your consent to process your Personal Data, you have the right to withdraw that consent.	This right only applies where we process Personal Data based upon your consent.

Right to complain to the relevant data protection authority If you think that we have processed your Personal Data in a manner that is not in accordance with data protection law, you can make a complaint to the data protection regulator. If you live or work in an EEA member state, you may complain to the regulator in that state.	This right applies at any time.