DAIKIN APPLIED EUROPE S.p.A.

Summary Document
relating to

Organisation and Management Model
Legislative Decree no. 231/2001

"Organisational Model"

Special Section L

Information technology crime and illegal data handling.

CONTENTS

1. INFORMATION TECHNOLOGY CRIME AND ILLEGAL DATA HANDLING

1.1 Introduction

The offences dealt with in this Special Part are referred to in art. 24bis of Legislative Decree no. 231/2001, introduced by Law 48/2008 ratifying and implementing the European Council Convention on information technology crime.

In addition, subsequently, Decree Law No. 105 of 21 September 2019, converted into Law No. 133 of 18 November 2019, established the so-called "national cyber security perimeter", aimed at ensuring a high level of security of the networks, information systems and IT services of the Public Administration, bodies and national operators, both public and private, on which the exercise of an essential function of the State depends and on the malfunctioning, interruption or improper use of which could result in prejudice to national security.

Relevant conduct, that may give rise to the direct administrative liability of the Company in whose interest or benefit the offence was committed, focuses on the offences described in the next paragraph.

In this regard, it is worth noting the sensitivity and relevance of the issue of computer crimes, taking into account in general the current spread of computer tools and the increase in attacks/violations of corporate information systems. Moreover, with the recent increase in the use of smart-working and the use of devices and/or personal network connections, companies are in general even more exposed to the risk of violation of the technical security measures adopted and therefore to the risk of committing the so-called computer crimes in question, which are relevant under Legislative Decree no. 231/01 if committed in the interest or to the advantage of the companies.

1.2 The types of offence

1.2.1 Illegal access to an information technology or telematic system

This offence, envisaged and punished by art. 615*ter* of the Criminal Code, relates to the behaviour of persons who gain illegal access to an information technology or telematic system protected by safety measures, or retains access thereto against the expressed or implicit wishes of those entitled to exclude said access. The offence is aggravated (i) if it is committed by a public official or by a person in public service, in abuse of the powers or in violation of the duties inherent in that function or service, or by a person illegally operating as a private investigator, or abusing their position as system operator; (ii) if the guilty party uses violence to persons or property in committing the offence, or if that party is obviously armed; (iii) if the fact results in the destruction or damaging of the system or a total or partial interruption in its operation, or the destruction or damaging of the data, information or programs it contains.

If the above facts relate to information technology or telematic systems of military interest or relating to public order or public security or health or civil defence or are in any case of public interest, the offence is further aggravated.

1.2.2 Illegal possession and distribution of information technology or telematic system access codes

This offence, which is foreseen and punished by art. 615*quater*, Criminal Code, relates to the actions of those who, in order to obtain profit for themselves or others or to cause injury to others, illegally procure, reproduce, distribute, communicate or hand over codes, passwords or other means of accessing an information technology or telematic system, protected by security measures, or in any way provide indications or instructions for that purpose.

1.2.3 Distribution of information technology programs, equipment or devices aimed at damaging or interrupting an information technology or telematic system

This offence, which is foreseen and punished by art. 615*quinquies*, Criminal Code, relates to the actions of those who, in order to illegally damage an information technology or telematic system, the information, data or programs it contains or pertaining to it, or favour the total or partial interruption, or alteration of its

operation, procure, produce, reproduce, import, distribute, communicate, deliver or in any way provide other information technology programs, equipment or devices.

1.2.4 Illegal interception, impediment or interruption of information technology or telematic communications

This offence, which is foreseen and punished by art. 617*quater*, Criminal Code, relates to the actions of those who fraudulently intercept communications relating to an information technology or telematic systems or between several systems, or impede them or interrupt them. Unless the offence represents a more serious crime, this type of offence also occurs when the contents of the above communications are revealed, either fully or in part, by means of any public information medium.

1.2.5 Installation of equipment to intercept, impede or interrupt information technology or telematic communications

This offence, which is foreseen and punished by art. 617*quinquies*, Criminal Code, relates to the actions of those who, outside the cases allowed by Law, install equipment capable of intercepting, impeding or interrupting communications relating to an information technology or telematic system or between several systems.

1.2.6 Damage to information technology programs, information and data

This offence, which is foreseen and punished by art. 635*bis*, Criminal Code, relates to the actions of those who, unless the offence represents a more serious crime, destroys, damages, deletes, alters or suppresses the information technology programs, information or data of others.

1.2.7 Damage to information technology programs, information and data used by the State or by another public body or that is of public utility

This offence, which is foreseen and punished by art. 635*ter*, Criminal Code, relates to the actions of those who, unless the offence represents a more serious crime, commits an action aimed at destroying, damaging, deleting, altering or suppressing information technology programs, information or data used by the State or by another public body or is of public utility.
The offence is aggravated if the action results in the destruction, damaging, deletion, alteration or suppression of the information technology programs, information or data.

1.2.8 Damage to information technology or telematic systems

This offence, which is foreseen and punished by art. 635*quater*, Criminal Code, relates to the actions of those who, unless the offence represents a more serious crime, by means of the actions indicated in article 635/bis, Criminal Code (cited above), or by the introduction or transmission of data, information or programs, destroys, damages, renders totally or partially useless the information technology or telematic systems of others, or seriously impedes their operation.

1.2.9 Damage to information technology or telematic systems of public utility

This offence, which is foreseen and punished by art. 635*quinquies*, Criminal Code, envisages an offence aggravated by the actions indicated in article 635/quater, Criminal Code (cited above) that occurs when the actions themselves are aimed at destroying, damaging, rendering totally or partially useless information technology or telematic systems that are of public utility, or seriously impeding their operation.

1.2.10 Falsification of a public information technology document or one used as evidence

This offence, under art. 491/bis, Criminal Code, envisages that if any of the falsifications relate to a public or private information technology document that is to be used as evidence, the provisions of the section relating to public documents and private agreements, respectively, shall apply.

1.2.11 Information technology fraud on the part of an individual providing electronic signature certification services

This offence, under art. 640*quinquies*, Criminal Code, envisages that the crime in question is committed by the individual providing electronic signature services who, in order to procure for himself or for others an illegal profit or to cause damage to others, violates the legal requirements for issue of a qualified certificate.

1.2.12 Violation of the rules on the National Cyber Security Perimeter (Art. 1, par. 11, Decree-Law No. 105/2019)

The offence is committed by any person who provides untrue information, data or factual elements relevant to the preparation or updating of the lists of networks, information systems and IT services used (Article 1(2)(b)), or for the purposes of prior communications to the National Assessment and Certification Centre or CVCN (Article 1(6)(a)), or for the performance of specific inspection and supervision activities (Article 1(6)(c)), or who fails to communicate such data, information or factual elements within the prescribed time limits.

1.1 The offences that are theoretically applicable to Daikin Applied Europe

OMISSIS

1.2 Sensitive activities

OMISSIS

1.3 The liabilities of the Company with regard to the illegal questions under analysis.

Daikin Applied Europe is committed to base its operations on criteria of maximum transparency and good faith, in compliance with applicable regulations and all other pertinent requirements. To that end, the Company has taken on the following commitments:

- involvement and awareness by the entire management structure, all employees and those who work on behalf of the organisation towards a culture of accountability and attention to questions regarding proper management of the company information technology and telematic system;
- ensuring that all activities are carried out in full compliance with the applicable legal requirements, and with all company rules aimed at preventing any risk of committing the offences indicated in Legislative Decree no. 231/01, with awareness among staff involved in processes considered to be sensitive of the potential risks of the offences set out in Legislative Decree no. 231/01 art. 24*bis*;
- the creation of suitable training operations for corporate staff regarding the potential risk of offences under Legislative Decree no. 231/01 art. 24*bis*;
- the provision of a disciplinary system to punish any failures to comply with the measures indicated in the Organisational Model in order to prevent the offences pursuant to art. 24 *bis* of Legislative Decree no. 231/01;
- the provision of suitable flows of information from employees to the Company Supervisory Body regarding all critical situations capable of resulting in a risk of committing offences under art. 24*bis*, Legislative Decree no. 231/2001.

Daikin Applied Europe also assures:

- that standardised corporate provisions and/or procedures have been set up to provide principles of behaviour, operating methods for carrying out sensitive activities, and suitable methods for storage of significant documentation;
- that all operations relating to sensitive activities are traceable, with particular reference to: ***i)*** registration of every operation; ***ii)*** ex post verification, if necessary using suitable documentary means, of the decision-making process, with reference to the reasoning behind each operational decision, to guarantee maximum transparency; ***iii)*** detailed regulation of the ability to delete or destroy the records taken;
- adequate segregation of tasks, insofar as possible, if necessary using a suitable system of proxies and powers of attorney, with separation of the activities of persons giving authorisation, persons performing tasks and persons controlling and with identification of an Officer in charge of sensitive activities;
- periodic performance, by the Officer in charge of sensitive activities, of monitoring actions and, when requested, preparation of the relevant reports and their transmission to the Supervisory Body, without prejudice to the general requirement of notifying the Company Supervisory Body of any tampering or illegal actions carried out on corporate information technology or telematic devices;
- a filing system for documentation relating to sensitive areas, that guarantees the impossibility of modifying the data contained therein (without said modifications being highlighted), and in which the filed documents can only be accessed by persons who have been authorised to do so under internal regulations;
- the adoption of a policy relating to information technology security, drawn up in advance, formally approved, updated periodically and communicated to all company staff;
- the adoption of backup procedures for each telecommunication network, as well as definition of the frequency of this activity, the manner in which it is carried out and the period for which the relevant data is stored;
- the existence of procedures to deal with possible emergency information technology events and/or disasters, by means of *incident tracking/incident handling* systems that are aimed, also by providing suitable communication channels and methods for timely signalling of incidents and suspicious situations, at tracing and storing and also managing all anomalies and suspicious situations that may occur during use of the information technology equipment, and guaranteeing timely intervention to solve the problem and prevent any further unsuitable behaviour;
- the existence of formalised procedures regarding the generation and protection of activity logs on the systems, at least as regards activities that involve sensitive data;
- the suitability of the human resources (both internal and external) involved in the IT area to cover their roles, in order to reduce risks deriving from actions liable to damage the integrity, confidentiality and use of the company information base, as well as the risks deriving from unauthorised use of the company information technology and information base. In particular, for this purpose the Company ensures i) that the adequacy, in terms of reliability and security, of the professional figures selected is verified, ii) that the responsibilities to be assigned to each resource are identified and the terms of the relevant working relationship, co-operation or consultancy are determined, iii) that relations with the selected resources are set down in written contracts, specifically highlighting the clauses relating to a description of the roles and responsibilities assigned, the confidentiality agreements and the controls that the Company reserves the right to perform on the relevant actions;
- management of relations with other parties according to principles of transparency, good practice and truthfulness;

- formalisation and documentation of the tasks assigned to external associates and consultants, highlighting the reasons for the choice of associate and/or consultant (also bearing in mind the type of activity assigned and the place in which it is to be carried out) and considerations on the price applied and on its coherence and congruence;
- control of the activity carried out, on behalf of the Company, by external associates and consultants, as well as on management and storage activities for the relevant documentation.

OMISSIS

1.4 Principles and rules of behaviour for Recipients

Recipients, identified in the light of the indications provided in the General Section (point 3.5), **must:**

- refrain from engaging in conduct liable to commit the offences pursuant to Legislative Decree no. 231/01;
- refrain from engaging in conduct that, although not covered within the meaning of Legislative Decree no. 231/01, have the potential to be considered as such;
- act in respect of the powers of representation and signature, within the scope of the duties and proxies conferred;
- behave in an ethical and transparent manner in all activities, in accordance with the law and internal company procedures;
- use company information technology tools, assigned in compliance with the company procedures in force, solely to carry out work activities;
- use internet browsing and electronic mail facilities solely for work activities;
- take due care of the credentials allowing access to the information technology systems used, ensuring that they do not come to the knowledge of third parties, and updating passwords periodically;
- take due care of company or third party information technology resources (e.g. desktop or laptop computers) used to carry out work activities;
- respect the security policies agreed and drawn up with third parties to access the systems or infrastructures of said third parties.

All the Recipients of this Model (identified pursuant to point 3.5 of the General Section), are subject to the following prohibitions, as general rules of behaviour:

- prohibition from implementing, co-operating in or causing behaviour that - when considered individually or collectively - falls either directly or indirectly within the types of offence taken into consideration above;
- prohibition from violating the company principles and procedures envisaged in this Special Section;
- prohibition from gaining unauthorised access to the information technology systems used by the Public Administration or from altering, in any way, their operation or intervening in any unauthorised way on the data, information or programs contained in an information technology or telematic system or pertaining thereto in order to obtain and/or modify information to the advantage of the company or of third parties, or in order to procure an undue advantage for the company or for third parties;
- prohibition from any conduct, including conduct with the assistance of third parties, aimed at accessing the information technology systems of other with the aim of illegally acquiring, damaging or destroying information or data contained therein;

- prohibition from illegally acquiring, altering, damaging or destroying information or data contained in company or third party information technology systems or the information technology programs of the Company or the Public Administration, in order to obtain advantages or favourable terms for the company;
- prohibition from destroying or altering information technology documents filed on the network directories or on company application software and, in particular, documents that might be considered evidence in a court of law;
- prohibition from damaging, destroying the archives or supports relating to back-up activities;
- prohibition from illegally holding, distributing or using codes giving access to the information technology or telematic systems of third parties or public bodies;
- prohibition from accessing the company network and programs using an identification code other than the one assigned;
- prohibition from revealing to anybody your authentication credentials (user name and password) giving access to the company network or to other sites/systems;
- prohibition from illegally intercepting, impeding or interrupting information technology or telematic communications;
- prohibition from installing, using, duplicating or distributing to third parties (software) programs without holding a proper license or exceeding the rights granted by the license held (e.g. maximum number of installations or users);
- prohibition from accessing restricted areas (such as server rooms, technical rooms, etc.) without adequate authorisation, either temporary or permanent;
- prohibition from accessing, for whatever purpose or use, without authorisation and in violation of the law, the information technology or telematic systems of others, and from violating the relevant access restrictions to the Company's corporate information technology system;
- prohibition, in general, except in the case of special authorisations deriving from specific working reasons, including access through automatic restriction or blocking systems, from connecting to, consulting, browsing, streaming and downloading from web sites considered to be illegal (and therefore, as an example, from sites whose contents are contrary to morals, religious freedom and public order, that allow violation of privacy, that promote and/or support terrorist or subversive movements, that relate to information technology piracy activities, or that violate copyright laws);
- prohibition from modifying the standard corporate settings of company software and hardware and those for connection of company information technology or telematic devices to public or private connection networks by means of instruments (telephone lines or wireless equipment) of any kind;
- prohibition from altering and/or modifying information technology documents that can be used as evidence;
- prohibition from avoiding the security rules imposed on corporate information technology or telematic instruments and on the internal connection networks.
- prohibition from creating falsified (both in terms of material and content) company documents of external significance;
- prohibition from leaving documents containing confidential information or system access codes unattended;
- prohibition from leaving own personal computers unattended and unlocked;

- prohibition from using the information technology systems available for unauthorised activities while carrying out working activities;
- prohibition from using corporate memory devices to store unauthorised content or files or those representing a violation of copyright.

1.5 Specific procedures

OMISSIS

1.6 Checks and information flow to the Supervisory Body

The Supervisory Body carries out periodic checks on the risk assets, indicated above, in order to verify consistency with the requirements contained in the Organisational Model and, in particular, with the procedures that the Company has established to govern the carrying out of sensitive activities.

All business functions, senior management and/or those subject to management by other parties, together with the members of the corporate bodies, have an obligation to promptly inform the Supervisory Body of any requests formulated or of the occurrence of events or circumstances such as to suggest the committing of a possible offence under Legislative Decree no. 231/2001.

OMISSIS