Techbau Green Energy S.p.A

Head office:
Via del Lago, 57
28053 Castelletto Sopra Ticino (NO) / Italy
Tel. +39 0323 589 500
info@tbge.it
www.tbge.it

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL OF TECHBAU GREEN ENERGY S.p.A.

in accordance with Legislative Decree 231/2001

Revision No. 3 – 19 December 2025

Techbau Green Energy S.p.A

Head office:
Via del Lago, 57
28053 Castelletto Sopra Ticino (NO) / Italy
Tel. +39 0323 589 500
info@tbge.it
www.tbge.it

REVISION HISTORY

REV.	DATE	DESCRIPTION OF CHANGES	PREPARED	CHECKED AND APPROVED
03	19 December 2025	Update	Giannangeli Consulich Legal advisors	Board of Directors of Techbau S.p.A.
02	15 December 2023	Update	Giannangeli Consulich Legal advisors	Board of Directors of Techbau S.p.A.
01	12 October 2022	First issue	Legal advisors	Board of Directors of Techbau S.p.A.

GENERAL SECTION

CONTENTS

1. RELEVANT LEGISLATION

1.1 Introduction

Legislative Decree No. 231 of 8 June 2001 (hereinafter also referred to as the “Decree” or “Legislative Decree 231/2001”), concerning the “Regulation of the administrative liability of legal persons, companies and other associative structures, including those without legal personality (so-called “Entities”), pursuant to Article 11 of Law No. 300 of 29 September 2000”, introduced for the first time in Italy a system of administrative liability for offences on the part of Entities, in addition to that of the natural person who actually committed the unlawful act, this was also done with a view to bringing domestic legislation on the liability of legal persons into line with certain international conventions to which Italy had long since acceded.

This is a new and broader form of administrative liability (essentially comparable to criminal liability), which holds organisations (meaning companies, associations, consortia, etc.) liable for offences committed, in their interest or to their advantage, by persons functionally linked to them (senior managers and persons subject to their management and supervision).

The Decree provides that legal entities may be held liable, and consequently penalised, for the commission of certain offences (so-called ‘predicate offences’) exhaustively listed in the law and contained in a schedule that is subject to amendment and supplementation by the legislature.

The first fundamental criterion for attributing liability is that the offence must have been committed in the interest or for the benefit of the organisation (the so-called ‘objective criterion’): this means that the organisation’s liability arises where the act was committed to benefit the organisation, without it being necessary for the result to have been actually and concretely achieved.

‘Advantage’ constitutes a ‘concrete acquisition of economic benefit’, whilst ‘“interest” implies only that the offence is aimed at securing that benefit, without, however, requiring that it be actually achieved’.

The organisation is therefore not liable if the offence was committed by one of the persons mentioned above in their own exclusive interest or that of a third party; indeed, the exclusive interest of the perpetrator or the third party does not give rise to any liability on the part of the organisation, as there is a break in the pattern of organic identification, given that the legal person is manifestly unconnected to the offence.

The second fundamental criterion for attribution, on the other hand, consists in the fact that the offence was committed by a natural person linked to the organisation by a functional relationship (the so-called ‘subjective’ criterion). In particular, the offence must have been committed by:

- persons “who hold representative, administrative or managerial functions within the organisation or within one of its organisational units endowed with financial and functional autonomy, as well as persons who, even de facto, exercise management and control over the organisation” (so-called ‘persons in senior positions’ or ‘Senior Persons’, such as, for example, the legal representative, the director, the general manager or persons who exercise, even de facto, the management or control of the organisation);

- “persons subject to the direction or supervision of one of the senior persons” (so-called “persons in a subordinate position” or “Subordinate Persons”, i.e. subordinates, typically employees, but also persons external to the entity, who have been entrusted with a task to be carried out under the direction and supervision of senior persons).

Whether the perpetrator of the offence belongs to one category or the other is decisive for the purposes of selecting the subjective criteria for attribution applicable to the specific case, which, depending on the different position within the organisation of the entity, are necessarily differentiated (see Articles 6 and 7 of the Decree).

If the offence was committed by a person in a senior position, the organisation’s liability is linked to the fact that ‘senior management expresses and represents the organisation’s policy’; for this reason, the organisation is identified with the natural person who acted for its benefit or in its interest.

If, on the other hand, the offence was committed by a person in a subordinate position, the entity’s liability is linked to its failure to comply with its management or supervisory obligations, and the offence depends on the existence of serious organisational shortcomings for which the entity may be held accountable (see Article 7 of the Decree). The attribution of the offence to the organisation presupposes, in any case, the existence (and therefore proof) of a causal link between the failure to comply with management and supervisory obligations and the criminal conduct of the subordinate individual, such that it is possible to attribute so-called ‘organisational fault’ to the organisation.

The liability of the organisation is linked to that of the actual perpetrator of the offence, but it is also direct and independent and does not depend on the establishment of liability on the part of a natural person (see Article 8 of the Decree).
Italian jurisdiction applies where the act or omission constituting the offence took place within the territory of the Italian State, or where the event resulting from such act or omission occurred in Italy (Article 6(2) of the Criminal Code).

Entities having their principal place of business within the territory of the State (the determination of which must be based on the civil law provisions applicable to legal persons and undertakings) are also liable for offences committed abroad, provided that no proceedings are brought against them by the State in which the offence was committed.

1.2 <u>Sanctions applicable to the organisation</u>

The system of sanctions set out in the Decree is based on a two-pronged approach: on the one hand, financial penalties; and on the other, disqualification orders.

The main and mandatory sanction is the financial penalty, imposed using a quota system: for each offence, there is a minimum and a maximum number of quotas, not less than 100 and not more than 1,000, and each quota corresponds to a sum of money ranging from €258.00 to €1,549.37. The judge determines the number of units based on the seriousness of the offence and the degree of liability of the organisation, as well as the measures taken by the organisation to eliminate or mitigate the consequences of the unlawful act and to prevent the commission of further offences. The amount of each unit, on the other hand, is set by the judge,

taking into account the organisation's financial and asset situation. The total amount of the financial penalty is therefore determined by multiplying the first factor (number of instalments) by the second (amount of each instalment).
In practice, therefore, financial penalties may range from a minimum of €258 (which may be reduced, pursuant to Article 12 of the Decree, by up to half) to a maximum of €1,549.

The financial penalty is of an administrative nature and is always imposed, even if the organisation has remedied the legal consequences arising from the offence.

The financial penalty shall be reduced by one third to one half if, prior to the opening of the trial at first instance:

- the organisation has fully compensated for the damage and has eliminated the harmful or dangerous consequences of the offence, or has in any event taken effective steps to that end;
- an organisational model suitable for preventing offences of the type that occurred has been adopted or made operational.

Furthermore, the financial penalty shall be reduced by half if:

- the perpetrator committed the offence primarily in their own interest or that of third parties, and the organisation derived no benefit or only a minimal benefit from it;
- the financial loss caused is particularly minor.

Disqualification sanctions, on the other hand, apply only to those offences for which they are expressly provided for and consist of:

- disqualification from carrying out the activity;
- the suspension or revocation of authorisations, licences or concessions necessary for the commission of the offence;
- a ban on contracting with the public administration, except for the provision of a public service (this ban may also be limited to certain types of contract or to certain public authorities);
- exclusion from benefits, funding, grants or subsidies and the possible revocation of those already granted;
- a ban on advertising goods or services.

Disqualification sanctions are characterised by their ability to restrict or impose conditions on a company's activities; in the most serious cases, they can bring the organisation to a standstill (prohibition on carrying out its activities) and may also be applied as precautionary measures prior to conviction (where there are serious grounds for believing that the organisation is liable for an administrative offence arising from a criminal offence, and there are well-founded and specific elements suggesting a real risk that offences of the same nature as the one under investigation will be committed).

Disqualification sanctions apply in the cases expressly provided for by the Decree where at least one of the following conditions is met:

- the organisation has derived a substantial profit from the offence and the offence was committed by persons in senior management positions or by persons under the direction of others and, in the latter case, the commission of the offence was caused or facilitated by serious organisational failings;
- in the event of repeated offences.

Disqualification sanctions shall have a duration of not less than three months and not more than two years and may be imposed on a permanent basis in the most serious situations described in Article 16 of the Decree (if the entity is used for the sole or predominant purpose of enabling or facilitating the commission of offences, or where the entity has already been convicted at least three times in the last seven years).

It should also be noted that the entity's activities may continue (instead of the sanction being imposed) under the supervision of a commissioner appointed by the court pursuant to Article 15 of Legislative Decree 231/2001, where one of the following conditions applies:

- the organisation provides a public service or a service of public necessity, the interruption of which could cause serious harm to the community;
- the interruption of the organisation's activities may, taking into account its size and the economic conditions of the area in which it is situated, have significant repercussions on employment.

In addition to these penalties, there are two further penalties:

- confiscation, which is always applied in the event of a conviction and relates to the proceeds or profit of the offence (except for the part that may be returned to the injured party), or, if this is not possible, sums of money or other assets of equivalent value to the proceeds or profit of the offence; this is without prejudice to rights acquired by third parties acting in good faith. The aim is to prevent the organisation from exploiting unlawful conduct for the purpose of 'profit'. Article 53 of the Decree provides for the possibility of ordering preventive seizure with a view to confiscation;
- the publication of the judgment, which may be ordered when a disqualification order is imposed on the organisation; the judgment is published once only, in extract form or in full, in one or more newspapers chosen by the judge, and by posting on the notice board of the local council where the organisation has its registered office. Publication is at the entity's expense and is carried out by the court registry; the aim is to bring the conviction to the public's attention.

1.3 <u>Predicate Offences</u>

The entity's liability may arise only from the commission of the offences expressly set out in the Decree. The list of offences has been gradually expanded since the Decree came into force and now encompasses a wide variety of offences.

Specifically, the offences to which the legislation applies are as follows:

a) Offences committed in dealings with the public administration and against the assets of the State or another public body (Articles 24 and 25 of the Decree):

- misappropriation of public funds (Article 316 bis of the Criminal Code);
- unlawful receipt of public funds (Article 316 ter of the Criminal Code);
- corruption (Articles 318, 319, 320, 321 and 322-bis of the Criminal Code);
- corruption in judicial proceedings (Article 319 ter of the Criminal Code);
- undue inducement to give or promise a benefit (Article 319 quater of the Criminal Code);
- incitement to corruption (Article 322 of the Italian Criminal Code);
- fraud to the detriment of the State or a public body (Article 640(2)(1) of the Italian Criminal Code);
- aggravated fraud to obtain public funds (Article 640 bis of the Italian Criminal Code);
- computer fraud to the detriment of the State or another public body (Article 640 ter of the Italian Criminal Code);
- trafficking in unlawful influence (Article 346-bis of the Italian Criminal Code);
- extortion (Article 317 of the Criminal Code);
- fraud in public procurement (Article 356 of the Italian Criminal Code);
- fraud against the European Agricultural Fund (Article 2 of Law 898/1986);
- embezzlement (Article 314 of the Italian Criminal Code), if the offence harms the financial interests of the European Union;
- misappropriation by taking advantage of another person's error (Article 316 of the Italian Criminal Code), if the offence harms the financial interests of the European Union;
- misappropriation of money or movable property (Article 314-bis of the Italian Criminal Code)
- interference with the freedom of tendering procedures (Article 353 of the Italian Criminal Code);
- interference with the freedom of the contractor selection procedure (Article 353-bis of the Italian Criminal Code).

b) Cybercrimes and unlawful processing of data (Article 24-bis of the Decree):

- falsification of public electronic documents or documents having probative value (Article 491-bis of the Italian Criminal Code);
- unauthorised access to a computer or telecommunications system (Article 615 ter of the Italian Criminal Code);
- unauthorised possession, distribution and installation of equipment, codes and other means designed to gain access to computer or telecommunications systems (Article 615 quater of the Italian Criminal Code);
- unlawful interception, obstruction or interruption of computer or telecommunications communications (Article 617 quater of the Criminal Code);
- unauthorised possession, distribution and installation of equipment and other means designed to intercept, obstruct or interrupt computer or telecommunications communications (Article 617 quinquies of the Italian Criminal Code);
- damage to information, data and computer programmes (Article 635 bis of the Italian Criminal Code);
- damage to information, data and computer programmes used by the State or by another public body or, in any event, for public benefit (Article 635 ter of the Italian Criminal Code);
- damage to computer or telecommunications systems (Article 635 quater of the Italian Criminal Code);

- unauthorised possession, distribution and installation of computer equipment, devices or programmes intended to damage or disrupt a computer or telecommunications system (Article 635-quater.1 of the Italian Criminal Code);
- damage to computer or telecommunications systems of public interest (Article 635 quinquies of the Italian Criminal Code);
- computer fraud committed by a person providing electronic signature certification services (Article 640-quinquies of the Criminal Code);
- failure to disclose, or the disclosure of false information, data or relevant facts concerning the national cyber security framework (Article 1(11) of Decree-Law No 105/2019);
- cyber extortion (Article 629(3) of the Italian Criminal Code).

c) Organised crime offences (Article 24-ter of the Decree):

- criminal association (Article 416 of the Italian Criminal Code);
- mafia-type organisations, including foreign ones (Article 416 bis of the Criminal Code);
- political-mafia electoral collusion (Article 416 ter of the Italian Criminal Code);
- kidnapping for the purpose of extortion (Article 630 of the Italian Criminal Code);
- criminal association for the purpose of illicit trafficking in narcotic or psychotropic substances (Article 74 of Presidential Decree 309/09);
- the unlawful manufacture, importation into the country, offering for sale, transfer, possession and carrying in a public place or a place open to the public of military or military-style weapons or parts thereof, explosives, illicit weapons, as well as common firearms (Article 407(2)(a)(5) of the Italian Criminal Code).

d) Offences relating to the forgery of currency, public credit instruments and revenue stamps (Article 25-bis of the Decree):

- counterfeiting of currency, the circulation and importation into the State, by prior agreement, of counterfeit currency (Article 453 of the Criminal Code);
- alteration of coins (Article 454 of the Criminal Code);
- the circulation of counterfeit coins received in good faith (Article 457 of the Italian Criminal Code);
- the circulation and importation into the country, without prior agreement, of counterfeit coins (Article 455 of the Criminal Code);
- counterfeiting of revenue stamps, bringing them into the country, purchasing, possessing or putting into circulation counterfeit revenue stamps (Article 459 of the Criminal Code);
- counterfeiting of watermarked paper used for the manufacture of public credit instruments or revenue stamps (Article 460 of the Italian Criminal Code);
- the manufacture or possession of watermarks or instruments intended for the counterfeiting of coins, revenue stamps or watermarked paper (Article 461 of the Criminal Code);
- use of counterfeit or altered revenue stamps (Article 464 of the Criminal Code);
- counterfeiting, altering or using trade marks or distinctive signs, or patents, models and designs (Article 473 of the Criminal Code);

- the importation into the country and trade in products bearing false marks (Article 474 of the Criminal Code).

e) Offences against industry and trade (Article 25 bis.1 of the Decree):

- interference with the freedom of industry or trade (Article 513 of the Criminal Code);
- unlawful competition involving threats or violence (Article 513 bis of the Italian Criminal Code);
- fraud against international industries (Article 514 of the Criminal Code);
- fraud in the conduct of trade (Article 515 of the Criminal Code);
- sale of non-genuine foodstuffs as genuine (Article 516 of the Criminal Code);
- sale of industrial products bearing false markings (Article 517 of the Criminal Code);
- manufacture and trade in goods produced by infringing industrial property rights (Article 517 ter of the Italian Criminal Code);
- counterfeiting of geographical indications or designations of origin of agri-food products (Article 517 quater of the Criminal Code).

f) Corporate offences (Article 25-ter of the Decree):

- false corporate disclosures (Articles 2621 and 2621-bis of the Civil Code);
- false corporate disclosures by listed companies (Article 2622 of the Civil Code);
- obstruction of supervision (Article 2625(2) of the Civil Code);
- unauthorised repayment of capital contributions (Article 2626 of the Civil Code);
- unlawful distribution of profits and reserves (Article 2627 of the Civil Code);
- unlawful transactions involving shares or equity interests in the company or its parent company (Article 2628 of the Civil Code);
- transactions to the detriment of creditors (Article 2629 of the Civil Code);
- failure to disclose a conflict of interest (Article 2629-bis of the Civil Code);
- fictitious formation of capital (Article 2632 of the Civil Code);
- unlawful distribution of company assets by liquidators (Article 2633 of the Civil Code);
- bribery between private individuals (Article 2635 of the Civil Code);
- incitement to corruption between private individuals (Article 2635-bis of the Civil Code);
- unlawful influence on the general meeting (Article 2636 of the Civil Code);
- market manipulation (Article 2637 of the Civil Code);
- obstruction of the functions of public supervisory authorities (Article 2638 of the Civil Code);
- false or omitted statements in relation to the issue of the preliminary certificate (Article 54 of Legislative Decree 19/2023).

Article 25-ter of Legislative Decree 231/2001 – in subparagraphs (d) and (e) – provides for the liability of the entity for the offence of false statements in a prospectus, whilst continuing to refer to the administrative offence referred to in Article 2623 of the Civil Code, paragraph 1 (Article 25-ter, subparagraph d) and the offence referred to in Article 2623, paragraph 2 of the Civil Code (Article 25-ter, subparagraph e), which have now been repealed. As a matter of prudence, we consider it appropriate to amend the Code of Conduct as if this reference were not merely formal – that is, directed solely at the offence of false statements in a prospectus as originally conceived in Article 2623 of the Civil Code – but were also intended to cover subsequent amendments to the penalties governing the offence in question, which is now regulated differently by Article 173-bis of the Consolidated Law on Finance (Legislative Decree 58/1998).

Furthermore, by virtue of the legislative amendments introduced by Legislative Decree 39/2010:

- Article 2624 of the Civil Code, concerning falsehoods in reports or communications by audit firms, has been repealed;
- Article 2625(1) of the Civil Code has been amended as follows:
    - the words ‘or auditing’ have been deleted;
    - the words: ‘to other corporate bodies or to audit firms’ are replaced by the following: ‘or to other corporate bodies’;
- the new offences of ‘false statements in reports or communications by statutory auditors’ (Article 27 of Legislative Decree 39/2010) and ‘obstruction of audit’ (Article 29 of the same decree) have been introduced.

Given the preventive nature of the criminal offences covered by this model, as a precautionary measure – and for the same reasons set out above regarding the repealed Article 2623 of the Civil Code – it is advisable to amend the model as if the entity’s administrative liability also applied to the commission of the new offences and the offences as now reformulated.

g) Offences committed for the purposes of terrorism or subversion of the democratic order (Article 25-quater of the Decree):

- subversive associations (Article 270 of the Criminal Code);
- associations with the aim of terrorism, including international terrorism, or subversion of the democratic order (Article 270-bis of the Criminal Code);
- aiding and abetting members (Article 270 ter of the Criminal Code);
- recruitment for the purposes of terrorism, including international terrorism (Article 270 quater of the Criminal Code);
- training for activities for the purposes of terrorism, including international terrorism (Article 270 quinquies of the Criminal Code);
- organising transport for the purposes of terrorism, including international terrorism (Article 270 quater.1 of the Italian Criminal Code);
- financing of conduct for the purposes of terrorism (Article 270 quinquies.1 of the Criminal Code);
- the removal of property or money subject to seizure (Article 270 quinquies.2 of the Italian Criminal Code);
- conduct for the purposes of terrorism (Article 270-sexies of the Criminal Code);
- an attack for terrorist or subversive purposes (Article 280 of the Criminal Code);
- acts of terrorism involving lethal devices or explosives (Article 280 bis of the Italian Criminal Code);
- acts of nuclear terrorism (Article 280 ter of the Criminal Code);
- kidnapping for the purposes of terrorism or subversion (Article 289-bis of the Criminal Code);
- kidnapping for the purpose of coercion (Article 289 ter of the Criminal Code)
- incitement to commit any of the offences set out in the first and second paragraphs (Article 302 of the Criminal Code);
- political conspiracy by agreement (Article 304 of the Criminal Code);
- political conspiracy by association (Article 305 of the Italian Criminal Code);

- armed gang: formation and participation (Article 306 of the Criminal Code);
- aiding and abetting participants in a conspiracy or an armed gang (Article 307 of the Criminal Code);
- seizure, hijacking and destruction of an aircraft (Article 1 of Law No. 342/1976);
- damage to ground installations (Article 2 of Law No. 342/1976);
- New York Convention of 9 December 1999 (Article 2);

h) Practices involving female genital mutilation (Article 583-bis of the Criminal Code) (Article 25-quater.1 of the Decree).

i) Offences against the individual (Article 25 quinquies of the Decree):

- enslaving or keeping a person in slavery or servitude (Article 600 of the Criminal Code);
- child prostitution (Article 600 bis of the Criminal Code);
- child pornography (Article 600 ter of the Criminal Code);
- possession of pornographic material (Article 600 quater of the Criminal Code), including virtual pornography (Article 600 quater.1 of the Criminal Code);
- tourism schemes aimed at the exploitation of child prostitution (Article 600 quinquies of the Italian Criminal Code);
- trafficking in human beings (Article 601 of the Italian Criminal Code);
- the purchase and sale of slaves (Article 602 of the Italian Criminal Code);
- unlawful labour brokering and exploitation (Article 603 bis of the Italian Criminal Code);
- solicitation of minors (Article 609 undecies of the Italian Criminal Code).

j) Offences relating to insider dealing and market manipulation (Article 25-sexies of the Decree):

- securities fraud (Article 512-bis of the Italian Criminal Code).

k) Offences relating to copyright infringement (Article 25 novies of the Decree):

- duplication, production, sale, hire, or importation into the territory of the State of computer programmes, database contents, and intellectual works (music, books, publications, etc.) (Articles 171, 171-bis, 171-ter, 171-septies and 171-octies of Law No. 633/1941).

l) Inducement to fail to make, or to make false, statements to the judicial authorities (Article 377 bis of the Criminal Code) (Article 25 decies of the Decree).

m) Environmental offences (Article 25 undecies of the Decree):

- environmental pollution (Article 452 bis of the Criminal Code);
- environmental disaster (Article 452 quater of the Criminal Code);
- environmental pollution and environmental disaster through negligence (Article 452 quinquies of the Criminal Code);
- trafficking in and abandonment of highly radioactive material (Article 452-sexies of the Criminal Code);

- criminal association and mafia-type association aggravated by the intention to commit environmental offences (Article 452-octies of the Criminal Code);
- organised activities for the illicit trafficking of waste (Article 452-quaterdecies of the Criminal Code);
- the killing, destruction, capture, removal or possession of specimens of protected wild animal or plant species (Article 727-bis of the Italian Criminal Code);
- destruction or deterioration of habitats within a protected site (Article 733-bis of the Italian Criminal Code);
- discharges of industrial waste water containing hazardous substances; discharges onto the ground, into the subsoil and into groundwater; discharges into the sea by ships or aircraft (Article 137 of Legislative Decree No. 152/2006);
- illegal dumping of waste in specific cases (Article 255-bis of Legislative Decree No. 152/2006);
- illegal dumping of hazardous waste (Article 255-ter of Legislative Decree No. 152/2006);
- unauthorised waste management activities (Article 256 of Legislative Decree 152/2006);
- unlawful incineration of waste (Article 256-bis of Legislative Decree No. 152/2006);
- pollution of the soil, subsoil, surface water or groundwater (Article 257 of Legislative Decree 152/2006);
- breach of obligations regarding reporting, the keeping of mandatory records and the completion of forms (Article 258 of Legislative Decree 152/2006);
- illegal trafficking of waste (Article 259 of Legislative Decree 152/2006);
- aggravating circumstance relating to business activities (Article 259-bis of Legislative Decree No. 152/2006);
- false information regarding the nature, composition and chemical-physical characteristics of waste when preparing a waste analysis certificate; entering a false waste analysis certificate into the SISTRI system; omission or fraudulent alteration of the hard copy of the SISTRI form – movement section relating to the transport of waste (Article 260-bis of Legislative Decree 152/2006);
- exceeding emission and air quality limit values (Article 279(5) of Legislative Decree 152/2006);
- breach of measures to protect stratospheric ozone and the environment (Article 3(6) of Law 549/1993);
- import, export, possession, use for profit, purchase, sale, display or possession for sale or for commercial purposes of protected species (Articles 1, 2, 3-bis and 6 of Law No. 150/1992);
- intentional or negligent pollution caused by a ship (Articles 8 and 9 of Legislative Decree 202/2007).

n) The offence of employing third-country nationals whose stay is irregular (Article 25-duodecies of the Decree).

- provisions against illegal immigration (Article 12, paragraphs 3, 3-bis, 3-ter and 5, of Legislative Decree No. 286/1998);
- employment of third-country nationals whose stay is irregular (Article 22(12-bis) of Legislative Decree No 286/1998).

o) Racism and xenophobia (Article 25 terdecies of the Decree):

- propaganda, instigation and incitement, based wholly or partly on the denial of the Holocaust or of crimes of genocide, crimes against humanity and war crimes (Article 3 of Law No. 654 of 13 October 1975).

p) Fraud in sporting competitions, the unauthorised operation of gambling or betting schemes, and gambling carried out using prohibited devices (Article 25 quaterdecies of the Decree):

- fraud in sporting events (Article 1 of Law No. 401 of 13 December 1989);
- unauthorised operation of gaming or betting activities (Article 4 of Law No. 401 of 13 December 1989).

q) 'Transnational' offences (Article 10 of Law No. 146 of 2006).

Article 10 of Law No. 146 of 16 March 2006 provides for the administrative liability of the organisation, limited to cases where the offences are of a 'transnational' nature within the meaning of Article 3 of the same law, for the following offences:

- criminal association (Article 416 of the Criminal Code);
- mafia-type association, including foreign ones (Article 416-bis of the Criminal Code);
- criminal association for the purpose of smuggling foreign manufactured tobacco (Article 291-quater of Presidential Decree No. 43 of 23 January 1973);
- criminal association for the purpose of illicit drug trafficking (Article 74 of Presidential Decree No. 309 of 9 October 1990);
- acts aimed at facilitating the illegal entry of a foreign national into the national territory and aiding and abetting their continued stay for the purpose of obtaining unlawful gain (Article 12(3), (3-bis), (3-ter) and (5) of Legislative Decree No. 286 of 25 July 1998);
- inducement to make no statement or to make a false statement to the judicial authorities (Article 377-bis of the Criminal Code);
- aiding and abetting (Article 378 of the Criminal Code).

r) Tax offences (Article 25 quinquiesdecies of the Decree):

- fraudulent declaration through the use of invoices or other documents relating to non-existent transactions (Article 2(1) of Legislative Decree No 74/2000);
- fraudulent declaration through the use of invoices or other documents relating to non-existent transactions, where the amount of the fictitious liabilities is less than €100,000.00 (Article 2(2-bis) of Legislative Decree 74/2000);
- fraudulent declaration by other means (Article 3 of Legislative Decree 74/2000);
- issuing invoices or other documents for non-existent transactions (Article 8(1) of Legislative Decree 74/2000);
- issuing invoices or other documents for non-existent transactions, where the false amount stated in the invoices or documents, per tax period, is less than €100,000.00 (Article 8(2-bis) of Legislative Decree 74/2000);
- concealment or destruction of accounting documents (Article 10 of Legislative Decree 74/2000);
- fraudulent evasion of tax payments (Article 11 of Legislative Decree 74/2000);
- making a false declaration (Article 4 of Legislative Decree 74/2000), if committed as part of cross-border fraudulent schemes involving the territory of at least one other Member State of the European Union and with the aim of evading VAT amounting to a total of not less than 10,000,000 euros;
- failure to submit a return (Article 5 of Legislative Decree 74/2000), if committed as part of cross-border fraudulent schemes involving the territory of at least one other Member State of the

European Union and with the aim of evading VAT amounting to a total of not less than 10,000,000 euros;

- unauthorised offsetting (Article 10-quater of Legislative Decree 74/2000), if committed as part of cross-border fraudulent schemes involving the territory of at least one other Member State of the European Union and with the aim of evading VAT amounting to a total of not less than 10,000,000 euros.

s) Smuggling offences (Article 25-sexiesdecies of the Decree):

- smuggling by failure to declare (Article 78 of Legislative Decree No. 141/2024)
- smuggling by making a false declaration (Article 79 of Legislative Decree No. 141/2024)
- smuggling in the movement of goods by sea, air and on border lakes (Article 80 of Legislative Decree No. 141/2024)
- smuggling through the unauthorised use of imported goods with total or partial remission of duties (Article 81 of Legislative Decree No. 141/2024)
- smuggling in the export of goods eligible for duty drawback (Article 82 of Legislative Decree No. 141/2024)
- smuggling in the context of temporary export and under the special use and processing arrangements (Article 83 of Legislative Decree No. 141/2024)
- smuggling of manufactured tobacco (Article 84 of Legislative Decree No. 141/2024)
- aggravating circumstances relating to the offence of smuggling of manufactured tobacco (Article 85 of Legislative Decree No. 141/2024)
- criminal organisation for the purpose of smuggling manufactured tobacco (Article 86 of Legislative Decree No. 141/2024)
- equating attempted offences with completed offences (Article 87 of Legislative Decree No. 141/2024)
- aggravating circumstances relating to smuggling (Article 88 of Legislative Decree No. 141/2024)
- evasion of the assessment or payment of excise duty on energy products (Article 40 of Legislative Decree No. 504/1995)
- evasion of the assessment or payment of excise duty on manufactured tobacco (Article 40-bis of Legislative Decree No. 504/1995)
- illicit manufacture of alcohol and alcoholic beverages (Article 41 of Legislative Decree No. 504/1995)
- conspiracy to illegally manufacture alcohol and alcoholic beverages (Article 42 of Legislative Decree No. 504/1995)
- evasion of the assessment and payment of excise duty on alcohol and alcoholic beverages (Article 43 of Legislative Decree No. 504/1995)
- aggravating circumstances (Article 45 of Legislative Decree No. 504/1995)
- tampering with devices, imprints and markings (Article 46 of Legislative Decree No. 504/1995).

t) Offences against cultural heritage (Article 25 septiesdecies of the Decree):

- theft of cultural property (Article 518 bis of the Criminal Code);
- misappropriation of cultural property (Article 518 ter of the Criminal Code);
- handling stolen cultural property (Article 518 quater of the Criminal Code);
- forgery of a private document relating to cultural heritage (Article 518-octies of the Criminal Code);
- unlawful importation of cultural property (Article 518 decies of the Criminal Code);
- unlawful removal or export of cultural property (Article 518 undecies of the Criminal Code);
- destruction, dispersal, deterioration, defacement, defiling and unlawful use of cultural or landscape heritage (Article 518 duodecies of the Italian Criminal Code);
- counterfeiting of works of art (Article 518 quaterdecies of the Criminal Code).

u) Money laundering involving cultural heritage and the devastation and looting of cultural and landscape heritage (Article 25 duodevicies of the Decree):

- money laundering involving cultural heritage (Article 518-sexies of the Criminal Code);
- destruction and looting of cultural and landscape heritage (Article 518 terdecies of the Criminal Code).

v) Offences against animals (Article 25-undevicies, Legislative Decree No. 231/2001)

- killing or causing harm to another person's animals (Article 638 of the Criminal Code);
- prohibition of animal fighting (Article 544-quinquies of the Italian Criminal Code);
- prohibited shows or events (Article 544-quater of the Italian Criminal Code);
- cruelty to animals (Article 544-ter of the Italian Criminal Code);
- killing of animals (Article 544-bis of the Criminal Code).

w) Attempting to commit any of the offences listed above (Article 26 of the Decree).

x) Offences committed abroad.

Pursuant to Article 4 of Legislative Decree 231/2001, the organisation may be held liable in Italy in relation to offences (covered by Legislative Decree 231/2001 itself) committed abroad.

The conditions on which the organisation's liability for offences committed abroad is based are:

- the offence must be committed abroad by a person functionally linked to the organisation, within the meaning of Article 5(1) of Legislative Decree 231/2001;
- the organisation must have its principal place of business within the territory of Italy;
- the organisation may be held liable only in the cases and under the conditions set out in Articles 7, 8, 9 and 10 of the Criminal Code;
- the organisation may be held liable in cases where the State in which the offence was committed does not bring proceedings against it;
- in cases where the law provides that the offender is to be punished at the request of the Minister of Justice, proceedings against the organisation shall be brought only if the request is also made against the organisation itself.

1.4 Forms of exemption from liability

In introducing the aforementioned regime of administrative liability, the Decree provides for a specific form of exemption from such liability where the body demonstrates that it has adopted all appropriate and necessary organisational measures to prevent the commission of offences by persons acting on its behalf. The existence of an adequate organisational structure is, therefore, both a measure and an indication of the organisation's diligence in carrying out its activities, with particular reference to those in which there is a risk of the offences provided for in the Decree being committed: the proven existence of an efficient and effective organisational structure therefore precludes the organisation's 'fault' and precludes the application of the relevant sanctions.

Specifically, the Board of Directors is responsible for adopting and effectively implementing the Organisation, Management and Control Model, in accordance with Article 6(1)(a), as well as for appointing the Supervisory Body, in accordance with the subsequent subparagraph (b).

Indeed, the organisation is exempt from penalty if it proves:

- that, prior to the commission of the offence, it had adopted and effectively implemented a model for organisation and management of crime-related risks suitable for preventing offences of the type that actually occurred (hereinafter the 'Model' or 'MOG');
- that it has entrusted the supervision of the functioning and compliance with the Model, as well as the task of ensuring its updating, to a body within the organisation endowed with autonomous powers of initiative and control (hereinafter the 'Supervisory Body' or 'OdV');
- that the persons who committed the offence did so by fraudulently circumventing the Model;
- that there was no omission or failure on the part of the Supervisory Body to exercise due supervision.

The organisation's liability is presumed if the offence is committed by a natural person holding a senior or managerial position; consequently, the burden of proving its lack of involvement in the events falls on the organisation. Conversely, the entity's liability must be proven where the person who committed the offence does not hold a senior position within the company's organisational structure; in such cases, the burden of proof lies with the prosecution.

If the offence was committed by persons subject to the management or supervision of one of the persons referred to above, the organisation is liable if the prosecution succeeds in proving that the commission of the offence was made possible by a failure to comply with management or supervisory obligations. These obligations are presumed to have been fulfilled if, prior to the commission of the offence, the organisation has adopted and effectively implemented a Code of Conduct suitable for preventing offences of the type that has occurred.

Article 6, paragraph 2, of the Decree sets out the content of the Model, which must have the following characteristics:

- identify the activities within which there is a possibility that the predicate offences may be committed;

- provide for specific protocols designed to plan the formulation and implementation of the organisation's decisions in relation to the offences to be prevented;
- identify methods for managing financial resources suitable for preventing the commission of such offences;
- set out obligations to report to the Supervisory Body;
- introduce an internal disciplinary system suitable for sanctioning failure to comply with the measures set out in the Model.

With regard to the effective implementation of the Model, the Decree also provides for the need for periodic review and amendment of the Model should significant breaches of the requirements be discovered or should changes occur in the organisation or activities of the entity.

The same Decree (Article 6(3)) provides that models may be adopted, whilst ensuring the above requirements are met, on the basis of codes of conduct (also referred to as guidelines) drawn up by representative trade associations.

The guidelines are submitted to the Ministry of Justice, which, in consultation with the relevant ministries, may, within 30 days, make observations on the suitability of the models drawn up in accordance with the trade associations' guidelines for preventing offences.

1.5 Confindustria Guidelines

In 2021, Confindustria updated its Guidelines for the development of organisational models.

The key points identified by the Guidelines for the development of organisational models can be summarised as follows:

- the identification of risk areas, aimed at highlighting the business functions within which the harmful events provided for in the Decree may occur;
- the establishment of a control system capable of preventing risks through the adoption of specific protocols. The most significant components of the control system devised by Confindustria are:
  - code of ethics;
  - organisational structure;
  - manual and IT procedures;
  - authorisation and signing powers;
  - integrated control and management systems;
  - communication with staff and staff training.

The components of the control system must be based on the following principles:

- verifiability, documentability, consistency and coherence of every transaction;
- application of the principle of segregation of duties (no one may manage an entire process independently);
- documentation of controls;
- provision of an appropriate system of sanctions for breaches of the code of ethics and the procedures/protocols set out in the model;
- identification of the requirements for the supervisory body, which can be summarised as:
  - autonomy and independence;
  - professionalism;

- continuity of operation;

- provision for procedures governing the management of financial resources;
- reporting obligations of the supervisory body.

Failure to comply with specific points of the Guidelines does not invalidate the Model, which must necessarily be drawn up with specific reference to the Company's actual circumstances, even if this means deviating from the Confindustria Guidelines, which, by their very nature, are of a general nature.

2. GOVERNANCE MODEL

2.1 Corporate governance system of Techbau Green Energy S.p.A.

Techbau Green Energy S.p.A. (hereinafter "Techbau Green Energy", the "Company") draws on the experience and 'energy' of Techbau S.p.A., a market-leading company in the construction sector which still holds the majority of its shares, and positions itself as a specialist partner in the development of green projects, with a particular focus on the construction and management of ground-mounted and rooftop photovoltaic systems, right through to the management of the energy produced under Power Purchase Agreements (PPAs).

Techbau Green Energy's range of renewable energy services stems from the need for environmental sustainability, inexhaustible energy sources linked to local conditions, and energy efficiency and independence. The services offered include: feasibility studies, energy management, trading, and facility management relating to the optimisation and installation of renewable energy systems.

Techbau Green Energy is a project company (also known as a special purpose vehicle, or SPV) established for the specific purpose of carrying out commercial, industrial and financial operations, relating to both movable and immovable property, deemed useful for the achievement of its corporate purpose; it may also acquire shareholdings in other companies or enterprises with a corporate purpose that is similar, related or connected to its own, within the limits of the law.

On 5 November 2025, the Company was converted from a limited liability company (S.r.l.) to a public limited company (S.p.A.), with Green 2 S.p.A. acquiring a minority stake of 49.9% in the share capital, a newly incorporated Italian vehicle, whose share capital is held by HoldCo, a subsidiary of the Eurizon Capital Real Asset SGR S.p.A. fund, acting in the name and on behalf of Eurizon Capital SGR S.p.A.

Techbau S.p.A., meanwhile, retains a majority stake of 50.01%.

Techbau Green Energy's corporate governance model is structured in such a way as to ensure and guarantee the Company maximum operational efficiency and effectiveness in carrying out its corporate activities. In particular, the Company is governed by a Board of Directors (hereinafter the "BoD") and oversight of management is entrusted to a Board of Statutory Auditors.

Techbau Green Energy does not have its own administrative structure and, at present, has a limited number of staff employed in administrative and commercial roles. For this reason, Techbau S.p.A. provides corporate and administrative services to Techbau Green Energy to enable it to achieve its corporate purpose. In this context, it contributes to the effective implementation of this Code through the procedures set out in greater detail in the document referred to **in Annex 1**.

2.2 's Control System

Techbau Green Energy S.p.A., in pursuing the objectives set out in its Articles of Association, has placed particular emphasis on the design and subsequent implementation of an appropriate control system, consistent with national and international best practices.

The control system aims to achieve the following objectives: (i) efficiency and effectiveness of operational activities; (ii) reliability of information; (iii) safeguarding of the company's assets; and (iv) compliance with laws and regulations to ensure accurate reporting and adequate control coverage across all activities, with particular attention to areas deemed to be at potential risk.

With this in mind, the Company is implementing audit and control processes aimed at obtaining the most relevant certifications in the areas of quality, the environment and safety.

With regard to activities involving a potential 'risk of offence' – within which, in principle, the offences set out in the Decree or, more generally, a breach of the Code of Ethics could be committed, as expressly identified below (hereinafter 'Activities at risk') – the Model provides for specific management and control protocols, under which Techbau Green Energy's organisational structure, supported by Techbau's resources, is to operate through formalised procedures designed to minimise the identified risks. In particular, the procedures set out in the Special Part of the Model comply with the following requirements:

- Explicit allocation of responsibilities
- Segregation of duties
- Traceability of processes through the production of specific documents
- Compliance with the principles of conduct set out in the Code of Ethics
- Integration with the procedures of the Integrated Management System (IMS)

The internal procedures established for the implementation of the protocols ensure, as far as possible given the size of the Company, the separation and hierarchical independence between those who make decisions, those who implement them and those responsible for carrying out checks.

Generally speaking, decisions of the Board of Directors of Techbau Green Energy may be adopted by written consultation or on the basis of consent expressed in writing, in accordance with the procedures laid down in the Company's Articles of Association. The shareholders decide on matters reserved to their competence by law and by the Company's Articles of Association, as well as on matters submitted for their approval by one or more directors or by shareholders representing at least one third of the share capital. Without prejudice to the specific provisions of the Company's Articles of Association, shareholders' decisions may also be adopted by written consultation or on the basis of consent expressed in writing; the Company's Articles of Association clarify, in fact, the circumstances in which shareholders' decisions must be adopted by resolution of the General Meeting.

Techbau Green Energy regards its Quality Management, Occupational Health and Safety, and Environmental Protection Management Systems as key tools for improvement. The significance of this message has been communicated to all staff through the following documents:

- "Quality Policy"
- "Health, Safety and Environment Policy"
- "Privacy and Information Security Policy"
- "Sustainability and Sustainable Procurement Policy"

The management systems incorporate the control activities necessary to verify compliance with the respective standards:

- UNI EN ISO 9001 for Quality Management Systems;
- UNI EN ISO 14001 for environmental management systems;
- UNI EN ISO 45001 for Occupational Health and Safety Management Systems;
- UNI EN ISO 27001: Information Security Management System.

2.3 Financial Resource Management Protocols

With regard to high-risk activities, the Model also provides for specific protocols governing the management of financial resources. The main purpose of these protocols is to prevent the creation of off-balance-sheet funds, not only in relation to Techbau Green Energy, but also to the other companies within the Group.

The company procedures established to implement these protocols ensure the separation and independence between those involved in making decisions on the use of financial resources, those who implement such decisions, and those entrusted with monitoring the use of financial resources.

All transactions involving the use or commitment of economic or financial resources must have an adequate justification and be documented and recorded, either manually or electronically, in accordance with the principles of professional and accounting integrity; the relevant decision-making process must be verifiable. All transactions relating to atypical or unusual activities or services must be specifically and clearly justified and reported to the Supervisory Body, in accordance with the procedure governing information flows to the Supervisory Body, which will be discussed below in the relevant section.

Exceptions to the protocols and procedures set out in the MOG are permitted in the event of an emergency or where it is temporarily impossible to implement them. The exception, with a clear statement of the reasons for it, must be reported to the line manager and the Supervisory Body.

3. THE MODEL ADOPTED BY TECHBAU GREEN ENERGY S.P.A.

3.1 Purpose of the Model

The Techbau Green Energy S.p.A. Model aims to prevent the commission of offences and to curb any unlawful conduct carried out in the course of the company's business, through the establishment of a structured and comprehensive system of procedures and control measures.

This objective is pursued by identifying the activities within which there is, to varying degrees, a risk of offences being committed. For each of these activities, the Company's organisational system imposes rules and processes designed to prevent offences from being committed, as well as an adequate internal control system.

Structured in this way, the Model aims to:

- clarify and define the conduct that is considered unlawful by the Company, as well as by the legal system, insofar as it contravenes the provisions of the law and the ethical principles that Techbau Green Energy intends to observe in the conduct of its business;
- inform and train all those acting in the name and on behalf of the Company that the commission of an offence (including attempted offences) – committed, in whole or in part, for the benefit or in the interests of the Company – constitutes a breach of company rules and may have criminal implications for them and administrative liability for the Company under Legislative Decree 231/2001;
- monitor the areas of activity where a risk of offences being committed has been identified.

3.2 Acceptable risk

A key concept in the development of the Model is that of acceptable risk. Indeed, for the purposes of applying the provisions of the Decree, it is important to define a threshold that sets a limit on the quantity and quality of the preventive measures to be introduced to deter the commission of offences.

With regard to the risk of offences under Legislative Decree 231/2001 being committed, the acceptability threshold is represented by a preventive system that cannot be circumvented except intentionally. In other words, in order for the organisation to be exempt from administrative liability, the persons who committed the offence must have acted by fraudulently circumventing the Model and the controls put in place.

3.3 The Model (structure, intended recipients and scope of application)

This Model consists of:

- a **'General** Section', which describes the relevant legislation and the general operating rules of the Model and the Supervisory Body;

- a "Special Part", focusing on the areas of activity and key processes deemed to be "at risk" and "sensitive", the rules of conduct and other control measures deemed relevant in relation to the offences to be prevented and the Company's organisational structure.

Should changes occur in the internal and external environment, the Company undertakes to adapt the Model and ensures its compliance and operation in accordance with the operational procedures deemed most appropriate, whilst respecting mandatory control principles.

The Model forms part of the broader organisational and control system of Techbau Green Energy S.p.A., which it is intended to complement with the following key elements:

- the mapping of activities at risk of the commission of offences under Legislative Decree 231/2001, to be subject to periodic analysis and monitoring;
- the rules of conduct, which are also set out in Techbau Green Energy S.p.A.'s Code of Ethics, aimed at preventing the commission of the offences referred to in Legislative Decree 231/2001;
- the assignment to the Company's Supervisory Body (OdV) of the tasks of overseeing the effective and proper functioning of the Model;
- the flow of information to the Supervisory Body;
- a system of sanctions designed to ensure the effective implementation of the Model, containing the disciplinary provisions applicable in the event of failure to comply with the measures set out in the Model itself;
- the verification and documentation of any atypical or significant transaction;
- the definition of authorisation and executive powers consistent with the assigned responsibilities;
- the provision to the Supervisory Body of company resources of a sufficient number and value, proportionate to the expected and reasonably achievable results;
- the rules and responsibilities for the implementation and periodic updating of the Model, as well as for verifying the functioning and effectiveness of the Model;
- activities to raise awareness, provide information and disseminate the rules of conduct and procedures adopted by the Company at all levels of the organisation and to external recipients;
- raising awareness and providing information to all those covered by the Code regarding compliance with the regulatory principles set out in the Decree.

The Code is specifically intended for the Company's Directors, employees and all persons who, in various capacities, are required to comply with and effectively implement the provisions set out therein (the "Recipients"). This refers, in particular, to employees of Techbau S.p.A. in the areas of responsibility identified in the contract referred to **in Annex 1** to this Code.

Where applicable, the Code is also intended for external collaborators, meaning both individuals and companies that, in various forms or ways, provide their services to Techbau Green Energy S.p.A. in the course of its business activities. Consequently, any such contracts that Techbau Green Energy S.p.A. may enter into with third parties must necessarily include specific clauses designed to ensure compliance with the Code or, in any event, compliance with Legislative Decree No. 231/2001.

In any event, before entering into binding contractual relationships with third parties, Techbau Green Energy must carry out an appropriate due diligence process aimed at verifying, amongst other things: (i) the reputation and reliability of the party with whom it intends to contract and of its key representatives, shareholders and directors; (ii) the financial and asset-relat ity and stability of the counterparty or partner; (iii) the technical competence and experience required to provide the service requested and covered by the contract; (iv) the references and relations with public authorities.

3.4 Approval of the Model

The Model, in accordance with the provisions of Article 6(1)(a) of the Decree, was adopted by the Company by a resolution of the Board of Directors dated 15 July 2023.

3.5 Updating and Implementation of the Model

The Model is subject to periodic review and is amended should any significant breaches of the requirements be identified or should there be changes to the organisation, the Company's activities or the relevant legislation.

Substantial amendments and/or additions to the Model, even where proposed by the Supervisory Body, fall within the remit of the Board of Directors.

Anyone working for or collaborating with the Company is required to comply with the relevant provisions of the Code, and in particular to observe the reporting obligations laid down to enable the monitoring of compliance of their actions with those provisions.

A copy of the Code, the documents annexed to it and any updates thereto is kept at the Company's registered office and is available to anyone authorised to consult it.

The Company shall notify each person required to comply with the Model of the relevant provisions relating to their specific activity or role.

As mentioned above, the Supervisory Body is responsible for monitoring the functioning, effectiveness and compliance with the Model, as well as for ensuring that it is kept up to date.

3.6 Model and Code of Ethics

Techbau Green Energy S.p.A. intends to base the conduct of its business, the pursuit of its corporate purpose and the growth of the Company on compliance not only with applicable laws and regulations, but also with shared ethical principles.

To this end, Techbau Green Energy S.p.A. has adopted a Code of Ethics (the "Code of Ethics"), approved by the Board of Directors at the same time as the Model was adopted, aimed at defining a set of principles of 'corporate ethics' which the Company recognises as its own and which it requires the corporate bodies and all those who contribute in any capacity to the pursuit of the Company's objectives to observe.

The Code of Ethics is of a general nature and represents a tool adopted independently by Techbau Green Energy S.p.A., although it refers to principles of conduct relevant to the Model.

4. THE SUPERVISORY BODY (OdV)

4.1 Composition

The Model provides for the establishment of an internal body, known as the Supervisory Body (OdV), which is entrusted with the task of continuously monitoring the effective functioning of and compliance with the Model, and of ensuring that it is kept up to date. The Supervisory Body must carry out specialist activities requiring knowledge of specific tools and techniques and must operate on a continuous basis. It cannot be part of the Board of Directors.

The Supervisory Body carries out its functions outside the Company's operational processes and is free from any hierarchical relationship within the company's organisational structure. The Supervisory Body reports directly to the Company's senior management, both operational and supervisory, so as to ensure its full autonomy and independence in carrying out the tasks entrusted to it.

The composition of the Supervisory Body is set out in the minutes of its appointment.

Techbau Green Energy S.p.A. designates a single-member body as the Supervisory Body, appointed by the Board of Directors from among individuals who are particularly qualified and experienced in matters relevant to Legislative Decree No. 231/2001, so as to ensure that the Body possesses adequate expertise in legal matters, risk assessment and internal auditing, as well as meeting the necessary integrity requirements.

The sole member of the Supervisory Body is independent of the Company and therefore:

- must not be linked to the Company or to its subsidiaries and/or associated companies, nor to its parent companies and/or shareholders, by an employment relationship or a consultancy or paid service arrangement, or by financial relationships that compromise their independence or imply, with regard to the Supervisory Body's areas of competence, potential conflicts of interest;
- it must not have any family ties with the shareholders or Directors of the Company, or of its subsidiaries and/or associated companies, or of its parent companies and/or shareholders, which could impair its independence of judgement;
- it has independent powers to take action within its areas of competence. To this end, and to ensure the continuous monitoring of the adequacy and suitability of the Model, the Supervisory Body makes use of internal staff and/or external consultants;

The Supervisory Body has its own Rules of Procedure.

The Supervisory Body has an expenditure budget for its exclusive use during the period in which it remains in office, as approved by the Board of Directors.

The Supervisory Body decides autonomously and independently on the expenditure to be incurred within the limits of the approved budget and refers the matter to those with signing authority at Techbau Green Energy S.p.A. to sign the relevant commitments. In the event of a request for expenditure exceeding the approved budget, the Supervisory Body must be authorised by the Board of Directors of Techbau Green Energy S.p.A.

The Supervisory Body is appointed for a term determined by the Board of Directors, with the possibility of renewal.

The Supervisory Body meets at least quarterly and, in any event, in accordance with the provisions set out in its own Rules of Procedure.

In order to gain a better understanding of and ensure proper oversight of the corporate environment, given the Company's simplified structure, the Supervisory Body may request that Directors attend its meetings to report on the Company's financial position. In such cases, the Directors attend the meetings solely as guests.

In general, in order to ensure effective and comprehensive oversight of corporate activities aimed at verifying and preventing the occurrence of significant risks within the meaning of Legislative Decree No. 231/2001, the Supervisory Body examines all corporate documentation relating to ordinary and extraordinary processes, which is provided to it by the Board of Directors in accordance with the provisions of paragraph 4.5 below.

The Supervisory Body also examines the documentation provided by Techbau S.p.A. and may liaise directly with the latter's employees regarding the work carried out on behalf of Techbau Green Energy S.p.A., as set out **in Annex 1.**

The following constitute grounds for ineligibility and incompatibility with the role of member of the Supervisory Body, including to ensure compliance with the requirement of good repute:

- holding the position of director of Techbau Green Energy S.p.A.;
- having conflicts of interest, even potential ones, with the Company such as to compromise one's independence;
- being married to, related by blood or by marriage up to the fourth degree to the persons referred to in the preceding points;
- having been convicted, even by a non-final judgement, to a custodial sentence entailing disqualification, even temporary, from public office or temporary disqualification from executive positions in ordinary legal entities;
- having been convicted, even by a non-final judgement and even following the application of a sentence on request pursuant to Articles 444 and 447 of the Code of Criminal Procedure, for intentional offences and for offences punishable on the grounds of intent or negligence as referred to in Legislative Decree No. 231/2001.

4.2 Revocation and Replacement

To safeguard the autonomy and independence of the Supervisory Body, changes to its structure (such as removals), its powers and its functioning may only be made by means of resolutions adopted by the Board of Directors with a duly reasoned vote and the unanimous consent of those present.

The Supervisory Body may only be dismissed for just cause.

In this regard, 'just cause' shall be understood to mean:

- a serious breach of its supervisory duties;
- a conviction of the Company or a plea agreement pursuant to the Decree, which establishes ‘failure to exercise supervision or insufficient supervision’ on the part of the Supervisory Body;
- a breach of confidentiality obligations (including those governed by Article 6, paragraph 2-bis, letter d) of Legislative Decree No. 231/2001).

In all cases where a disqualification sanction provided for by the Decree is applied as a precautionary measure, the Board of Directors, having obtained the necessary information, may, where appropriate, proceed to dismiss the Supervisory Body if it finds that there has been a failure to exercise supervision or that such supervision was insufficient.

Should the requirements of autonomy, independence and professionalism cease to be met, or should any of the grounds for ineligibility or incompatibility identified above arise, the Board of Directors, having carried out the necessary investigations and heard the person concerned, shall set a deadline, of not less than 30 days, by which the situation of incompatibility must cease. If this deadline expires without the aforementioned situation having been resolved, the Board of Directors must declare that the member of the Supervisory Board has been removed from office.

Similarly, a serious illness rendering a member of the Supervisory Body unfit to perform their supervisory duties, or an illness or other personal reasons which, in any event, result in their absence from the Supervisory Body’s activities for a period exceeding three months, shall result in a declaration of their removal from office, to be carried out in accordance with the procedures described above.

In the event of the resignation, dismissal or removal of a member of the Supervisory Body, the Board of Directors must appoint a replacement in a timely manner and until the new Supervisory Body is appointed.

4.3 Requirements

Regardless of its composition, the Supervisory Body must meet the following requirements:

- autonomy and independence: these aim to ensure that the Supervisory Body is not directly involved in the management activities that form the subject of its supervisory role and, above all, that it is able to carry out its role without direct or indirect influence from the entities it supervises. These requirements are ensured by the absence of any hierarchical reporting lines within the company’s organisation, the absence of operational tasks, and the power to report directly to the Board of Directors;
- professionalism: it is a body equipped with the technical, professional and specialist skills appropriate to the functions it is required to perform (e.g. interview techniques, flow charting, risk analysis techniques, etc.). These characteristics, combined with independence, guarantee objectivity of judgement;
- continuity of operation: it is a body within the organisation, adequately structured and resourced, and free from operational duties that might limit the commitment required to carry out its assigned functions;
- good repute and the absence of conflicts of interest.

In order to ensure that the Supervisory Body has the necessary capacity to obtain information and thus to act effectively within the company, the flow of information to and from the Supervisory Body is established through this Model and, subsequently, through specific internal organisational documents issued by the Board of Directors or the Supervisory Body.

4.4 Functions and Powers

The Supervisory Body, which reports directly to the Company's management body and has its own budget, is granted autonomous powers of initiative and control in the exercise of its functions; it may not be assigned operational tasks or decision-making powers – not even of a restrictive nature – relating to the conduct of the Company's business.

The Supervisory Body of Techbau Green Energy S.p.A. is generally entrusted with the task of monitoring:

- compliance with the provisions of the Model by the corporate bodies, consultants and counterparties, to the extent required of each;
- the effectiveness and adequacy of the Model in relation to the company's structure and its actual capacity to prevent the commission of the offences referred to in Legislative Decree 231/2001;
- whether the Model needs to be updated, should the need arise to adapt it in light of changes in the company's circumstances and/or regulatory requirements;
- the adequacy, application and effectiveness of the sanctions system.

At an operational level, the Supervisory Body is entrusted with the task of:

- carry out the monitoring activities provided for in the Model;
- constantly verifying the effectiveness and efficiency of current company procedures;
- carry out reviews of the company's activities with a view to updating the mapping of sensitive activities and instrumental processes;
- carry out periodic targeted checks on certain transactions or specific acts carried out by Techbau Green Energy S.p.A., particularly in the context of activities that are sensitive or 'instrumental' to their implementation;
- monitor initiatives to promote awareness and understanding of the Model and prepare the internal documentation necessary for the Model's operation, containing instructions, clarifications or updates. As part of its ongoing activities, the Supervisory Body must establish and apply operational procedures to ensure the best possible formal management of its activities;
- to collect, process and retain relevant information regarding compliance with the Model, as well as to update the list of information that must be provided to it or kept at its disposal, thereby constituting the 'formal' archive of internal control activities;
- verify the adequacy of the internal control system in relation to current legislation for the purposes of compliance pursuant to Legislative Decree No. 231/2001;
- to verify that the elements envisaged for the implementation of the Model (adoption of standard clauses, completion of procedures, etc.) are in any event adequate and meet the requirements for compliance with the provisions of the Decree, and, if this is not the case, to adopt or recommend the adoption of an update to those elements;
- to assess whether the Model requires updating;

- report periodically to the Board of Directors on the implementation of company policies for the implementation of the Model;
- to check the actual existence, proper maintenance and effectiveness of the records supporting the activities under Legislative Decree No. 231/2001;
- request that the Board of Directors provide all corporate documentation, the minutes of Board meetings, the documents through which the decisions of the Board of Directors are implemented, and contracts entered into by the Company.

To this end, the Supervisory Body is vested with the following powers:

- to issue provisions designed to regulate the activities of the Supervisory Body;
- to carry out inspections in accordance with procedures established in advance and communicated to the management body;
- to access any and all company documents relevant to the performance of the functions assigned to the Body pursuant to Legislative Decree No. 231/2001;
- to request information from anyone acting on behalf of the Company in the context of high-risk activities, even without prior authorisation from the management body;
- to engage external consultants of proven professional standing where this is necessary for the performance of verification and control activities or for updating the Model;
- to require the Board of Directors to promptly provide the information, data and/or details requested by them in order to identify aspects relating to the various business activities relevant under the Model and to verify its effective implementation;
- to express an opinion on the adequacy and suitability of amendments to the Model drawn up on the initiative of the management body, prior to their adoption.

4.5 Information flows from the Supervisory Board

The Supervisory Body reports the results of its monitoring activities directly to the Board of Directors and is not hierarchically subordinate to any of the company's departments.

Following each inspection, the Supervisory Body draws up a specific report, which is kept on file by the Body itself.

In particular, the Supervisory Body operates in accordance with the following reporting lines:

1. on a regular basis, by submitting an annual report directly to the Board of Directors and the Board of Statutory Auditors, and for information to the independent auditors;
2. promptly, by sending a report directly to the Chief Executive Officer and/or the Board of Directors and, in any event, to the Board of Statutory Auditors, where facts of particular significance are ascertained.

The Supervisory Body may be convened at any time by the Board of Directors or may, in turn, submit requests to that effect in order to report on the functioning of the Model or on specific situations.

Meetings with the individuals and bodies indicated above must be minuted; copies of the minutes shall be kept by the Supervisory Body and by the bodies involved on each occasion.

The Supervisory Body is informed of the Company's establishment of additional, independent reporting channels and of the need to liaise with the respective managers should it receive reports falling within their remit.

4.6 Information flows to the Supervisory Body

Requests for information and reports, as well as reports of breaches of the Code of Ethics, must be sent to the Supervisory Body at the email address *giannangeli@gecleg.it*

In accordance with the above provisions, with the adoption of this Model, the Company has established a specific procedure ("Information Flows to the Supervisory Body", **Annex 2**), involving the managers specified therein and setting out the subject matter and frequency of communication.

Reports of breaches of the Model may be sent to the Supervisory Body's email address indicated above, or by using the so-called 'whistleblowing' procedure with the safeguards provided for therein, as set out in paragraph 5 below, at the discretion of the reporting person.

4.7 Coordination with the Supervisory Body of Techbau S.p.A.

Following the adoption and implementation of the Code, regular dialogue will be ensured between the Supervisory Body and that of Techbau S.p.A., given that the latter provides corporate and administrative services to Techbau Green Energy to enable it to fulfil its corporate purpose.

In particular, it will be the responsibility of the Supervisory Body of Techbau S.p.A. to promote and ensure the effectiveness of such coordination, for example by scheduling meetings involving both Supervisory Bodies, with a view to facilitating the exchange of information on key issues such as any regulatory updates that may have occurred, problematic factors identified in the operation of the individual organisational models, and staff training.

5. WHISTLEBLOWING REPORTS

5.1 Introduction

The adequacy and effectiveness of the Code of Ethics and the Model depend, amongst other things, on the existence of an effective system for detecting unlawful conduct and breaches, enabling any infringements to come to light.

This framework was first implemented by Law 179/2017, which sets out provisions for the protection of persons reporting offences or irregularities of which they have become aware in the course of a public or private employment relationship (so-called 'whistleblowing'), and most recently by Legislative Decree 24/2023, through which Italy transposed Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national legal provisions.

More specifically, Legislative Decree 24/2023 stipulates that the Policy must contain provisions relating, amongst other things, to:

- internal reporting channels;
- external reporting channels;
- prohibitions on retaliation;
- the provision of an appropriate disciplinary system to sanction non-compliance with the measures set out in the Policy.

Under the recent reform, companies are generally required – depending on their size, whether they are public or private, and whether they have adopted an Organisational Model – to put in place appropriate mechanisms for receiving reports, including anonymous ones, from within or outside the organisation, relating to matters that may constitute administrative, accounting, civil or criminal offences; unlawful conduct as defined under Legislative Decree No. 231/2001; breaches of the Organisational Model; and acts or omissions that harm the financial interests of the European Union or relate to the internal market.

The scope of the report varies depending on the type of entity involved. With specific reference to the private sector, the legislation has been summarised in the Guidelines for External Reports adopted by ANAC on 12 July 2023, as set out below:

Given the private nature of the organisation and the fact that it employs fewer than 50 staff members, the Company is therefore required to implement an internal reporting channel for reports relating to breaches of Legislative Decree 231/2001 and this Organisational Model.

In accordance with the law, the management of the reporting channel must be entrusted either to a person or to a dedicated, independent internal department with staff specifically trained to manage the reporting channel, or to an independent external body with specifically trained staff. As also recognised by the ANAC Guidelines of 12 July 2023 and reiterated by the Confindustria Guidelines of 27 October 2023, this role may also be fulfilled by the Supervisory Body.

5.2 Scope of application

Form and content of reports

Reports may be made in writing (including electronically) or orally.

A report is defined as any communication, including anonymous reports, describing conduct (whether by action or omission) relating to members of the administrative and supervisory bodies, staff (managers, middle managers and employees) and third parties, in respect of which there is a reasonable suspicion or knowledge that such conduct is unlawful or carried out in breach of the Code of Ethics, the Model, the company's internal regulations or the relevant compliance procedures and/or standards pursuant to Legislative Decree 231/2001.

Reports must be detailed and based on factual evidence, and must be precise and consistent.

In particular, and for the purposes of assessing admissibility, the following essential elements of the report must be clear:

- the reporting person's identification details (first name, surname, place and date of birth), as well as a contact address to which subsequent updates may be sent;
- the time and place at which the incident forming the subject of the report occurred, i.e. a description of the facts forming the subject of the report, specifying the details relating to the circumstantial evidence and – where possible – the manner in which the reporting person became aware of the facts forming the subject of the report;
- personal details or other information enabling the identification of the person to whom the reported facts relate.

It is also helpful to attach documents that may provide evidence supporting the facts reported, as well as to indicate other individuals who may be aware of the facts.

In the case of a report sent by ordinary post, the whistleblower should also expressly state that they wish to benefit from whistleblowing protections (e.g. by including the phrase 'for the attention of the report handler only').

The following are excluded from the scope of reports:

- complaints, claims or requests relating to the whistleblower's personal interests that concern exclusively their own employment relationship or that relate to working relationships with superiors (e.g. labour disputes, discrimination, interpersonal conflicts between colleagues, reports concerning data processing carried out in the context of an individual's employment relationship where there is no harm to the public interest or to the integrity of the private organisation or public administration). Complaints excluded on the grounds that they relate to the whistleblower's personal interest are therefore not considered whistleblowing reports;
- matters relating to national security and defence;

- reports concerning breaches already subject to mandatory regulation in certain specialised sectors, to which the ad hoc reporting framework therefore continues to apply (financial services, anti-money laundering, terrorism, transport safety, environmental protection).

Applicability of the Regulations

All members of the Company, whether senior management or not, and third parties acting in any capacity on behalf of or in the interests of the Company, are under an obligation to report any breaches – even merely 'suspected' ones – of the Code of Ethics, the Model and the operating procedures of which they become aware, on pain of disciplinary sanctions.
A report may therefore be made by any person who has obtained information regarding potential offences within the workplace, including, by way of example only, employees, contractors, members of the board of directors, management or supervisory body, volunteers, trainees, contractors and subcontractors, suppliers, former employees whose employment has ended – provided the information was obtained whilst they were employed – or candidates who have not yet been hired, provided the information on the breaches was obtained during the recruitment process or at other pre-contractual stages.

Protected persons

The provisions on whistleblowing protect the following persons:
- employees of the Company;
- self-employed persons and those in a collaborative relationship who carry out their work at the Company;
- workers and collaborators carrying out their work for entities that supply goods or services or carry out works on behalf of the Company;
- freelancers and consultants who provide services to the Company;
- any volunteers and trainees, whether paid or unpaid, who carry out their work at the Company;
- persons holding administrative, managerial, supervisory, oversight or representative roles within the Company, even where such roles are exercised de facto, such as members of the Board of Directors, the Board of Statutory Auditors and the Supervisory Body.

The protection of whistleblowers referred to in the preceding paragraph also applies:
- where the legal relationship has not yet commenced, if the information on the breaches was obtained during the selection process or at other pre-contractual stages;
- during the probationary period;
- following the termination of the legal relationship, if the information regarding the breaches was nevertheless obtained during the course of that relationship.

The protective measures provided for in this Procedure also apply:
- to facilitators, defined as individuals who assist a whistleblower in the reporting process, working within the same workplace and whose assistance must be kept confidential;
- to persons in the same workplace as the whistleblower or linked to them by a stable emotional bond or kinship up to the fourth degree;
- to the whistleblower's work colleagues with whom they have a regular and ongoing relationship.

5.3 Internal reporting channel

Appointment of the person responsible

The Company designates the person responsible for establishing, implementing, managing and monitoring the internal reporting channel (hereinafter the "Whistleblowing Officer") as a member of the Company's single-member Supervisory Body, who is granted autonomy and has received specific and adequate training in the management of reports.

The Company, on the one hand, undertakes to guarantee the autonomy and independence of the Whistleblowing Officer and, on the other hand, the latter has a duty to ensure at all times that they are in a position to carry out investigations and, in general, to perform their duties independently of other company functions, that they are not subject to interference of any kind in the performance of these duties, and that they have all the necessary personnel and material resources to carry them out. Therefore, should the report itself or the subsequent investigation reveal circumstances suggesting the existence of a conflict of interest – even if only potential – involving the Whistleblowing Officer, he or she shall be required to refrain from any further activity relating to that report.

A conflict of interest may arise where the Whistleblowing Officer is the same person as the whistleblower, the person against whom the report is made, or is otherwise a person involved in or affected by the report.

In such situations, the report is addressed to the Chair of the Board of Directors, who is required to comply with the duty of confidentiality set out in the regulations.

Establishment of the reporting channel

The Company brings its reporting channel into line with the standards prescribed by current legislation, so as to make it accessible not only to employees but also to all other stakeholders, such as suppliers and existing or potential customers, and to ensure the confidentiality of the identity of the whistleblower, the person mentioned in the report and the contents of the report, in accordance with the terms set out below.

Reports may be submitted:

- **in writing via the online platform:** accessible via the Techbau Green Energy S.p.A. website: https://www.techbau.it/

- **in writing by post** to the following address:

  Elio Giannangeli, Solicitor
  Piazza Castello, 21
  20121 – Milan,

  The report must be placed in two sealed envelopes: the first must contain the reporter's personal details, together with proof of identity, and the second must contain the subject matter of the report. Both envelopes must be placed inside a third envelope bearing the words 'for the attention of the report handler' on the outside.

- **orally via an online platform:** accessible via the Techbau Green Energy S.p.A. website: https://www.techbau.it/, by attaching voice recordings.

As indicated above, it should be noted that the whistleblower is free to use this channel as the first point of contact to request an appointment, so that they may report the matter orally in person or, subject to agreement, remotely via online video-communication platforms.

Should the whistleblower request to make an oral report in person, the Whistleblowing Officer shall arrange an appointment within fifteen days, so that the whistleblower may report the matter in person or, subject to agreement, remotely via online video-communication platforms. In the case of a deferred oral report:

- a suitable location is identified to ensure the whistleblower's confidentiality;
- the whistleblower is informed that the conversation will be recorded;
- if the whistleblower objects to the recording, the Whistleblowing Officer shall draw up a specific report, signed by the whistleblower, and a copy shall be provided to them;
- the whistleblower will have the opportunity to review, correct and sign to confirm the transcript of the conversation.

Details of the reporting channel used are published on the Company's website and on the online noticeboard of the corporate intranet.

Should the whistleblower prefer not to reveal their identity, they may make an anonymous report. In such cases, it will nevertheless be necessary to identify the individuals involved in the reported incidents, in order to ensure that the investigation arising from the report is as effective as possible. In all cases, anonymous reports must be recorded by the Whistleblowing Officer and the documentation received must be retained; should the anonymous whistleblower subsequently be identified and have suffered retaliation, they must be afforded the protections provided for whistleblowers. The Whistleblowing Officer therefore guarantees the strictest confidentiality in such cases as well.

Handling of the report

In accordance with Article 5 of Legislative Decree 24/2023, once a report has been received, the Whistleblowing Officer shall:

- issue an acknowledgement of receipt to the whistleblower within seven days of receiving the report, except in the case of anonymous reports where it is in no way possible to identify the whistleblower and/or establish a channel of communication with them (e.g. an anonymous report sent by post in which no contact details have been provided to which any necessary correspondence may be sent);
- maintains contact with the whistleblower and, where necessary, requests further information from them;
- diligently follows up on the reports received;
- provides a response to the report within three months of the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months of the expiry of the seven-day period following the submission of the report. In particularly complex cases, the Whistleblowing Officer shall inform the whistleblower within the aforementioned period that the investigation is still ongoing.

The Whistleblowing Officer is also required to notify the other members of the Supervisory Body of the report.

With specific reference to point (c), the Whistleblowing Officer shall assess, including on the basis of any documentary analysis, whether the conditions for commencing the subsequent investigation phase are met, resulting in:

- the commencement of the preliminary investigation, if the report is admissible;
- closure of the report, if the report is deemed inadmissible, with a specific indication of the reason.

For the purposes of admissibility, the report must clearly set out:

- the time and place at which the incident forming the subject of the report occurred, through a description of the facts forming the subject of the report that includes details of the circumstantial evidence and, where applicable, the manner in which the whistleblower became aware of the facts;
- the personal details or other information enabling the identification of the person to whom the reported facts are attributed.

Conversely, the report is deemed inadmissible in the event of:

- a lack of the information constituting the essential elements of the report;
- the factual elements relating to the offences defined by law are manifestly unfounded;
- the presentation of facts of such a general nature that they cannot be understood by the Whistleblowing Officer;
- the submission of documentation alone, without an actual report of breaches.

Should the Whistleblowing Officer decide not to initiate the preliminary investigation, they shall inform the whistleblower within three months of the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months of the expiry of the seven-day period following the submission of the report. If the whistleblower cannot be contacted because the report is anonymous, the case shall be closed.

Reports closed on the grounds that they are manifestly unfounded, even if anonymous, are forwarded to the Head of HR so that appropriate action may be taken, in particular to assess whether they were made for the sole purpose of damaging the reputation or harming, or otherwise causing prejudice to, the person and/or the Company concerned.

<u>Conduct of the preliminary investigation</u>

During the preliminary investigation phase, the Whistleblowing Officer:

- carries out in-depth investigations and specific analyses aimed at verifying whether the reported breach has a reasonable basis;
- reconstructs the management and decision-making processes, based on the documentation and any further evidence it deems necessary;
- requests any further information or clarification from the person making the report;
- obtains any information from the relevant company departments and from the persons involved in the report, who may request a hearing or submit written comments or documents;
- obtains any information from the individuals involved in the report, including those whom the report holds responsible for the alleged breaches. These individuals (i) must be involved at the appropriate

time and in the appropriate manner to ensure the proper conduct of the investigation, and (ii) have the right to be heard and to submit written comments or documents. Should they be interviewed in person, these individuals are informed that the conversation will be recorded or set out in a specific report, which the complainant will have the opportunity to review, correct and accept by signing, without, however, receiving a copy;

- it formulates any recommendations regarding the adoption of the necessary remedial actions aimed at correcting any control deficiencies, anomalies or irregularities identified in the company areas and processes examined.

Should technical expertise not possessed by the Whistleblowing Officer prove necessary or even merely advisable for the analysis and proper handling of the report, the Whistleblowing Officer is authorised to be assisted by external consultants with proven experience and professionalism. These external consultants, as well as all those involved in the preliminary investigation, are also bound – subject to specific notification by the Whistleblowing Officer and the signing of appropriate documents where required – by the confidentiality obligations set out in more detail below.

In any event, should it prove necessary to seek technical assistance from third-party professionals, as well as specialist support from staff in other company departments, the Whistleblowing Officer is required to redact any data that could enable the identification of the whistleblower or any other person involved, unless such data is necessary for the investigation being conducted by those parties.

It is understood that assessments of merit or appropriateness – whether discretionary or technical-discretionary – relating to decision-making and management aspects carried out by the various company departments do not fall within the scope of the preliminary investigation, except where such assessments are manifestly unreasonable.

All stages of the preliminary investigation must be documented and archived, depending on the type of reporting channel used.

<u>Conclusion of the preliminary investigation</u>

Once the investigation has been completed and a decision has been taken on its outcome, the whistleblower is informed of the outcome of the investigation or of the need to continue the investigation. In the latter case, the whistleblower is subsequently informed of the actual closure of the investigation and its outcome.

With specific reference to the nature of this notification, the Whistleblowing Officer informs the whistleblower that the report (a) has been closed as it was deemed unfounded; or (b) has been brought to the attention of the relevant bodies within the Company, together with all the information and details necessary for them to take the appropriate measures.

The Whistleblowing Officer is not, in fact, responsible for assessing individual liability or any subsequent measures and/or proceedings that may arise.

Upon completion of each investigation, after having notified the whistleblower and, where appropriate, having consulted with the person against whom the report was made or assessed the written comments submitted by that person, the Whistleblowing Officer draws up a report for the Company's Board of Directors and the Supervisory Body, which sets out:

- a detailed description of the reported facts and the individuals involved;
- the facts established as a result of the investigation and the manner in which the investigation was conducted;
- the evidence gathered, including recordings of interviews, any written statements obtained or minutes of interviews, as well as any other relevant documentation;
- the conclusions reached following the preliminary investigation and, therefore, (a) an indication of any alleged non-compliance with provisions or procedures, or facts of disciplinary or employment law significance, as well as (b) any observations and recommendations regarding the necessary corrective actions to be taken.

The whistleblower's personal details or any other information that would allow their identification are not included, unless they have given their explicit consent.

Good faith in reporting

Reports must be made in good faith.

Whistleblowers acting in good faith are those who report or disclose breaches with a reasonable belief that the information reported is true or that it has been provided in accordance with the requirements set out in Legislative Decree 24/2023 and this procedure.

Submission of the report

Anyone who receives, in any form, a report that may be classified as whistleblowing (e.g. the term 'whistleblowing' is explicitly stated on the envelope, in the subject line or in the text of the communication) is required to forward the original, together with any supporting documentation, to the Whistleblowing Officer within seven days of receipt via the reporting channels described above, and to notify the whistleblower of the forwarding at the same time, if known.

To the person receiving the report:

- it is prohibited to retain a hard copy of the report;
- must delete any digital copies;
- is prohibited from undertaking any independent investigation or further examination of the report;
- you are obliged to maintain the confidentiality of the identity of the whistleblower, of the persons involved or otherwise mentioned in the report, of the content of the report and of the related documentation.

Failure to report a matter, as well as any breach of the duty of confidentiality, may result in the disciplinary measures set out in this Code being taken.

Information and Awareness-Raising

To ensure the proper and efficient functioning of the reporting system, it is necessary to promote a culture of whistleblowing within the Company.

To this end, the Company shall, through appropriate training, inform and raise awareness amongst employees regarding the reporting system adopted, setting out in a simple and understandable manner the purposes and procedures for using the internal reporting channel.

5.4 Confidentiality and protection of personal data

The internal reporting channel must guarantee the confidentiality of the whistleblower's identity and that of any other persons involved in the report, as well as the content of the report and the related documentation.

Any processing of personal data must be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree 196/2003 and Legislative Decree 51/2018. In any event, the report is exempt from the access provisions set out in Articles 22 et seq. of Law 241/1990, as well as Articles 5 et seq. of Legislative Decree 33/2013.

The processing of personal data will be carried out by the Whistleblowing Officer in their capacity as Data Controller solely for the purposes of implementing the procedures set out in this Policy and, therefore, for the proper management of reports received.

A privacy notice regarding the processing of personal data is published on the Company's website.

Reports may not be used beyond what is strictly necessary to follow them up. For this reason, personal data that is clearly not relevant to the processing of a specific report is not collected or, if collected accidentally, is deleted immediately.

The Whistleblowing Officer monitors compliance with organisational and technical measures designed to ensure the confidentiality of the whistleblower and the integrity and confidentiality of the information reported; He or she also ensures the security of the reporting channel in terms of the confidentiality, integrity and availability of information, both with regard to the details of the report and the identity of the whistleblower, even in the event that the report should subsequently prove to be incorrect or unfounded.

No form of threat, retaliation, sanction or discrimination against the whistleblower, the person against whom the report is made, or anyone who has assisted in investigating the validity of the report will be tolerated.

Subject to legal obligations, the identity of the whistleblower and any other information from which their identity may be inferred, directly or indirectly, may not be disclosed, without their express consent, to persons other than those authorised to receive or follow up on reports, who are expressly authorised to process such data pursuant to Articles 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196/2003.

To achieve these objectives, the Whistleblowing Officer carries out annual risk assessments relating to the protection of personal data, taking into account the five-year time limit, starting from the date of notification of the outcome of the procedure, for the retention of the data covered by the report.

The identity of the whistleblower and any other information from which that identity may be deduced, directly or indirectly, may only be disclosed with the whistleblower's express consent:

- as part of disciplinary proceedings, where the allegation appears to be well-founded on the basis of the report and knowledge of the whistleblower's identity is essential for the defence of the accused;
- in proceedings initiated as a result of the report, where the disclosure of the whistleblower's identity or any other information from which that identity may be deduced, directly or indirectly, appears to be essential also for the purposes of the defence of the person concerned.

The reasons for disclosing confidential information shall be communicated in writing to the whistleblower in advance. Should the whistleblower withhold their consent, the report may not be used in the disciplinary proceedings, which therefore may not be initiated or continued in the absence of further evidence on which to base the allegation.

In any event, the obligation to protect the whistleblower may be waived if:

- the whistleblower gives their express consent to the disclosure of their identity;
- the whistleblower's identity must be disclosed to the judicial authorities, the Public Prosecutor or another competent authority in the context of a criminal, disciplinary or regulatory investigation;
- the whistleblower's criminal liability for the offences of slander or defamation, or in any event for offences committed in connection with the report, has been established by a first-instance judgment; or their civil liability has been established in cases of wilful misconduct or gross negligence;
- anonymity is not enforceable by law and the whistleblower's identity is requested by the judicial authority.

Any breach of the duty of confidentiality may result in ANAC imposing administrative fines on the person concerned, as well as the adoption of the disciplinary measures provided for in this Code.

5.5 Prohibition of Retaliation

It is prohibited to take any retaliatory action against the whistleblower, defined as any conduct, act or omission – including any attempt or threat thereof – carried out as a result of the internal report which causes or may cause the whistleblower, directly or indirectly, unjust harm.

The prohibition on retaliation against the whistleblower covers a range of cases, including, but not limited to:

- dismissal, suspension or equivalent measures;
- demotion or failure to be promoted;
- a change of duties, a change of workplace, a reduction in salary, or a change in working hours;
- suspension from training or any restriction on access to it;
- negative performance appraisals or negative references;
- the imposition of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;

- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including the loss of economic opportunities and loss of income;
- inclusion on inappropriate lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in that sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the revocation of a licence or permit;
- a requirement to undergo psychiatric or medical examinations.

The Company shall take appropriate action against anyone who carries out or threatens to carry out acts of retaliation against those who have made reports in accordance with the provisions set out in this Code, without prejudice to the right of the relevant parties to seek legal redress should the reporter be found liable, whether criminally or civilly, for false statements or reports.

Any acts of retaliation taken as a result of the report are null and void, and persons who have been dismissed as a result of the report are entitled to be reinstated in their job.

ANAC is the authority responsible for receiving and handling reports from whistleblowers regarding alleged acts of retaliation suffered by them.
In order for this form of protection to be recognised:

- the whistleblower, at the time of making the report, lodging a complaint with the judicial or accounting authorities, or making a public disclosure, must have reasonable grounds to believe that the information is true and falls within the scope of the relevant legislation;
- the report, complaint or disclosure must have been made in accordance with the provisions of Legislative Decree 24/2023 and this Procedure.

Any retaliation arising from the report constitutes a very serious breach which may result in ANAC imposing administrative fines on the Company ranging from 10,000 to 50,000 euros.

Without prejudice to ANAC's exclusive competence regarding the possible imposition of the administrative sanctions referred to in Article 21 of Legislative Decree 24/2023, the Company may take the most appropriate disciplinary and/or legal measures to protect its rights, assets and reputation against anyone who, acting in bad faith, has made false, unfounded or opportunistic reports for the sole purpose of defaming or causing harm to the person reported or to other individuals mentioned in the report.

It remains, however, within the remit of the judicial authorities to order the necessary measures to ensure the protection of the whistleblower (e.g. reinstatement to their post, compensation for damages, an order to cease the conduct, and a declaration of nullity of the measures taken).

As already stated, the whistleblower loses this protection:

- if the whistleblower's criminal liability for the offences of defamation or slander is established, even by a first-instance judgment, or if such offences are committed in connection with the report made to the judicial or accounting authorities;
- in the event of civil liability on the same grounds due to wilful misconduct or gross negligence.

In such cases, the whistleblower is subject to a disciplinary sanction.

Protection, albeit belated, must nevertheless be afforded even in the event of a first-instance judgement not upheld on appeal, the case being dismissed, or where minor negligence has been established.

5.6 Limitations on liability

In accordance with the provisions of Legislative Decree 24/2023, the whistleblower cannot be held liable, either criminally, civilly or administratively:

- for the disclosure and use of official secrets (Article 326 of the Criminal Code);
- for the disclosure of professional secrecy (Article 622 of the Italian Criminal Code);
- for the disclosure of scientific and industrial secrets (Article 623 of the Italian Criminal Code);
- breach of the duty of fidelity and loyalty (Article 2105 of the Civil Code);
- breach of the provisions relating to the protection of copyright;
- breach of the provisions relating to the protection of personal data;
- disclosure or dissemination of information regarding infringements that damage the reputation of the person concerned.

The above limitations on liability apply only where:

- at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to expose the reported breach;
- the report is made in accordance with the conditions required to benefit from protection against retaliation (reasonable grounds to believe the reported facts to be true, the infringement is one that can be reported, and the procedures and conditions for submitting the report are complied with).

In any event, liability is not excluded for conduct which:

- is not related to the report;
- is not strictly necessary to disclose the breach;
- constitute the unlawful acquisition of information or access to documents.

Where such acquisition constitutes a criminal offence (e.g. unauthorised access to a computer system or an act of hacking), the whistleblower remains liable under criminal law and is subject to any other civil, administrative and disciplinary liability. Conversely, the extraction (by copying, photographing or removal) of documents to which the whistleblower had lawful access is not punishable.

5.7 Sanctions system

The disciplinary system set out in this Code also applies to those responsible for retaliation, obstruction (including attempted obstruction) of reporting, breach of confidentiality obligations, failure to establish reporting channels, or the adoption of reporting procedures that do not comply with the provisions of Legislative Decree 24/2023.

The whistleblower may also report to ANAC any retaliation they believe they have suffered, and ANAC, in the cases set out in the preceding points, is required to impose the following administrative fines on the person responsible:

- from 10,000 to 50,000 euros, where it ascertains that retaliation has taken place, that the report has been obstructed or that an attempt has been made to obstruct it, or that the duty of confidentiality has been breached;
- from 10,000 to 50,000 euros, where it ascertains that reporting channels have not been established, that procedures for making and managing reports have not been adopted, or that the adoption of such procedures does not comply with current legislation, as well as where it ascertains that the verification and analysis of reports received have not been carried out;
- from 500 to 2,500 euros, in the cases referred to in Article 16(3) of Legislative Decree 24/2023, unless the whistleblower has been convicted, even at first instance, of the offences of defamation or slander or, in any event, of the same offences committed in connection with the report made to the judicial or accounting authorities.

6. SELECTION, INFORMATION AND TRAINING OF STAFF

6.1 Staff selection

The selection and management of employees, as well as of Techbau Green Energy's suppliers and business partners, must comply with criteria of reasonableness, professionalism, integrity, fairness and transparency, in accordance with the Company's Code of Ethics, and taking into account the company's requirements in relation to the application of Legislative Decree 231/2001.
In particular, Techbau Green Energy's staff are subject, even at the initial selection stage, to an assessment process of their skills and performance that takes into account both technical and soft skills.

The Supervisory Body, in coordination with the relevant company departments, analyses the specific candidate assessment system used during the selection process, which is drawn up by the Company on the basis of business needs and in compliance with the provisions of Legislative Decree 231/2001.

6.2 Staff Information

To ensure the effectiveness of this Model, the Company aims to guarantee the proper dissemination and understanding of the rules of conduct contained herein amongst both existing staff and new recruits, with varying degrees of detail depending on the level of involvement of the staff concerned in high-risk activities.

The information and ongoing training system is supervised and supplemented by the work carried out in this area by the Supervisory Body, which oversees operations in collaboration with the relevant company departments and the heads of the departments involved from time to time in the application of the Model.

This Model is communicated to all staff members within the Company at the time of its adoption. To this end, a hard copy of the Model and the Code of Ethics is displayed on the company noticeboard, and a digital copy of the Code of Ethics is published on the company website.

New recruits are informed of the existence of the aforementioned noticeboard and are also provided with a hard copy of the aforementioned Code.

The Model will form part of the training programme described in the following paragraph.

6.3 Staff training

The training programme, which aims to raise awareness of the legislation set out in Legislative Decree 231/2001, varies in terms of content and delivery methods depending on the role of the participants, the level of risk in the area in which they operate, and whether or not they hold a representative role within the Company.

It is the responsibility of the various company departments to:

- to draw up a regular refresher programme to be shared with Techbau Green Energy's Supervisory Board, which, in accordance with the provisions of the Model, sets out a specific programme for managerial staff and for subordinate staff;

- draw up a timetable to be communicated, together with a summary of the programme's content, to the Supervisory Board.

Conversely, it shall be the responsibility of the Supervisory Board to inform the various company departments regarding:

- changes to the relevant legislation that require supplementary training;
- the need for supplementary training following the identification of errors or deviations from the correct execution of operational procedures applied to so-called 'sensitive activities'.

Training will be provided to all persons responsible for the effective implementation of this Model, with the aim of raising awareness of the legislation referred to in Legislative Decree 231/2001.

By way of example only, the following are considered to be information-providing activities:

- the organisation of regular sessions;
- the distribution of training materials;
- discussions conducted by the Supervisory Body to ascertain actual knowledge of the Model, including through the completion of assessment questionnaires.

7. DISCIPLINARY SYSTEM

7.1 General Principles

Pursuant to Article 6(2)(e) and Article 7(4)(b) of Legislative Decree 231/2001, organisational, management and control models may be considered effectively implemented only if they provide for a disciplinary system capable of sanctioning non-compliance with the measures set out therein.

This disciplinary system must apply both to employees and to third parties acting on behalf of or in conjunction with the Company, providing for appropriate sanctions of a disciplinary nature, on the one hand, and of a contractual or contractual-negotiated nature, on the other.

The application of disciplinary sanctions is independent of the initiation or outcome of any criminal proceedings, as the Organisational Models and internal procedures constitute binding rules for those subject to them, the breach of which must be sanctioned regardless of whether an offence has actually been committed or is punishable. The principles of promptness and immediacy of sanctions mean that delaying the application of disciplinary sanctions pending the outcome of criminal proceedings is not only unnecessary but also inadvisable.

7.2 Sanctions against employees and managers

This Code constitutes, to all intents and purposes, a set of company regulations, reflecting the employer's authority to issue instructions regarding the performance and discipline of work.

The Company's disciplinary code, adopted in accordance with current legislation and national and regional sectoral collective agreements, is supplemented by the provisions set out below.

The following constitute disciplinary offences by an employee or manager of the Company:

- failure to document, or the incomplete or untruthful documentation of, the work carried out, as specifically required for high-risk activities;
- failure to document, retain and monitor the records and activities provided for in the control protocols, with the aim of preventing the transparency and verifiability of those activities;
- obstructing audits, or unjustifiably preventing access to information and documentation by those responsible for auditing procedures and decisions, including the Supervisory Body, or other conduct likely to breach or circumvent the control system, such as the destruction or alteration of documentation required by the Model;
- the omission or breach, even if isolated, of the protocols and requirements of the Model designed to ensure health and safety in the workplace;
- repeated and unjustified breaches of other protocols of the Model (for example, failure to comply with prescribed procedures, failure to provide the Supervisory Body with the requested information, failure to carry out checks, or conduct that does not comply with the requirements of the Model itself);
- breach of confidentiality obligations, failure to establish reporting channels, adoption of reporting procedures that do not comply with the provisions of the Decree, and engaging in retaliatory conduct

against whistleblowers or obstructing (even if only attempted) the reporting process (as discussed below).

Disciplinary sanctions, graded according to the seriousness of the breach, are imposed on the employee or manager, including following a report and request from the Supervisory Body, in accordance with applicable statutory and contractual provisions.

The type and severity of each of the sanctions referred to above must take into account the principles of proportionality and appropriateness in relation to the alleged breach. These sanctions will therefore be applied in relation to:

- the intentional nature of the conduct (in the case of wilful misconduct) or the degree of negligence, imprudence or incompetence with regard to the foreseeability of the event (in the case of negligence);
- the significance of the obligations breached;
- the employee's overall conduct, with particular regard to the existence or otherwise of previous disciplinary records, within the limits permitted by law;
- the level of hierarchical and/or technical responsibility of the persons involved in the alleged conduct;
- the actual or potential consequences for the Company;
- other specific circumstances surrounding the disciplinary breach;
- whether an intentional or negligent offence has actually been committed as a result of the breach of a protocol or procedure.

For the purposes of any aggravation (or mitigation) of the sanction, the following factors are also taken into account:
professional conduct, previous work performance, previous disciplinary records, and the circumstances in which the offence was committed;

- behaviour immediately following the incident, with particular reference to any active repentance;
- whether multiple breaches were committed as part of the same conduct, in which case the sanction applicable to the most serious breach shall be imposed;
- whether several individuals were involved in committing the breach;
- any repeat offence by the perpetrator.

The application of the sanctions set out in the following points shall in no way prejudice the Company's right to take action against the person responsible in order to obtain compensation for all damages suffered as a result of or in consequence of the established conduct.

The Company imposes disciplinary sanctions in accordance with the procedures set out in Article 7 of Law 300/1970 (the so-called Workers' Statute) and any special regulations, in accordance with the disciplinary framework set out in the relevant National Collective Labour Agreement currently in force.

By way of example:

a) an employee who commits minor acts or omissions in breach of the internal procedures set out in this Code (for example, if they fail to follow the prescribed procedures, fail to provide the Supervisory Body with the necessary information, fail to carry out their monitoring duties, etc.) or, whilst carrying out high-risk activities, behaves in a manner that does not comply with the requirements of the Code;

b) a fine may be imposed on an employee who repeatedly fails to comply with the internal procedures set out in this Code or who, whilst carrying out high-risk activities, repeatedly behaves in a manner that does not comply with the requirements of the Code;
c) an employee who, by failing to comply with the internal procedures set out in this Code or by adopting, whilst carrying out high-risk activities, behaviour that does not comply with the provisions of the Model, commits acts that expose the Company to an objective situation of danger or acts contrary to the Company's interests, such behaviour being deemed to cause damage or a situation of danger to the integrity of the Company's assets;
d) an employee who, whilst carrying out high-risk activities, adopts conduct that does not comply with the provisions of this Code and which results in the commission of an offence provided for by the Decree shall be dismissed with compensation in lieu of notice, as such conduct shall be deemed to cause significant damage or a situation of significant prejudice to the Company;
e) an employee who, whilst carrying out high-risk activities, adopts conduct that is a clear breach of the provisions of this Code, such that it results in the actual imposition on the Company of measures provided for by the Decree, may be subject to dismissal without notice.

7.3 Measures in respect of employees, suppliers, business partners and consultants

Any conduct on the part of the Company's collaborators, suppliers, business partners and consultants that contravenes the provisions of Legislative Decree 231/2001 or this Code may result in the imposition of penalties or, in the event of serious breach, the termination of the contractual relationship, without prejudice to any claim for compensation should such conduct result in damage to the Company, even independently of the termination of the relationship.

To this end, contracts entered into by the Company with third parties must contain an explicit reference to the existence of the Model and the Code of Ethics, and must include specific clauses acknowledging the third-party contractor's knowledge of the Model, the Code of Ethics and the Decree, and providing for the Company's right to terminate the relationship in the event of breaches by the third party. Furthermore, the third party – and its employees and collaborators – must explicitly undertake to refrain from conduct that could constitute the predicate offences and to adopt appropriate control systems.

7.4 Measures concerning Directors and Statutory Auditors

Breaches of the Code committed by persons who hold, or who de facto exercise, functions of representation, administration or management of the Company or of one of its organisational units with financial and functional autonomy, or who exercise control functions within the Company, shall be reported by the Supervisory Body to the Board of Directors for the appropriate decisions to be taken and, for information, to the Board of Statutory Auditors.

7.5 Breaches relating to whistleblowing

With regard to breaches relating to whistleblowing, the ANAC Guidelines of 12 July 2023 – which are incorporated in this respect by the Confindustria Guidelines of 27 October 2023 – distinguish, for the purposes of identifying the party liable, between natural and legal persons deemed responsible and therefore subject to the sanction, depending on the specific circumstances.

In particular:

- in cases where the reporting channel has not been established, where procedures have not been adopted, or where non-compliant procedures have been adopted, the responsible party is identified as the governing body;
- in cases where the verification and analysis of reports received have not been carried out, as well as where the duty of confidentiality has been breached, the responsible party is identified as the Whistleblowing Officer.

The handling of reports falls within the remit of the Whistleblowing Officer's duties. Any breaches therefore entail the application of the sanctions set out in the National Collective Agreement, where applicable.

With regard, however, to sanctions against those who have engaged in retaliatory acts, the individual identified as responsible for the retaliation is subject to sanctions.

Specifically, the administrative fines are as follows:

- from 10,000 to 50,000 euros where it is established that the individual identified as responsible has committed acts of retaliation;
- from 10,000 to 50,000 euros where it is established that the natural person identified as responsible has obstructed the reporting of the matter or has attempted to do so;
- from 10,000 to 50,000 euros where it is established that the natural person identified as responsible has breached the duty of confidentiality referred to in Article 12 of Legislative Decree 24/2023. This is without prejudice to the sanctions applicable by the Data Protection Authority for matters falling within its remit under the legislation on personal data;
- from 10,000 to 50,000 euros where it is established that no reporting channels have been set up. In such cases, the governing body is deemed to be liable;
- from 10,000 to 50,000 euros where it is established that no procedures have been adopted for the handling and management of reports, or that the adoption of such procedures does not comply with the provisions of the decree. In such cases, the governing body is deemed liable;
- from 10,000 to 50,000 euros where it is established that the received reports have not been verified and analysed. In such cases, the Whistleblowing Officer is held liable;
- from 500 to 2,500 euros, where the civil liability of the whistleblower for defamation or slander is established, including by a first-instance judgment, in cases of wilful misconduct or gross negligence, unless the whistleblower has already been convicted, including at first instance, of the offences of defamation or slander or, in any event, of the same offences committed in connection with the report made to the judicial authorities.