CODE OF ETHICS

BOUYGUES

CONTENTS

EDITORIAL

The efficiency and future of the Bouygues group depend on the confidence the Group inspires in its customers, its employees, its shareholders and its private- and public-sector partners. We can only ensure our development by adopting a fair, honest attitude towards them.

This confidence is created, in particular, by compliance with the rules of conduct that I have frequently reiterated in recent years. After consulting the Ethics, CSR and Patronage Committee of the Bouygues Board of Directors, I decided in 2006 to combine these rules in a Code of Ethics, which is made accessible to each Group employee. The Code is updated regularly.

In this Code, the Group undertakes to comply with the strictest standards when doing business. This Code should help in mobilising our organisational structures and improving our conduct. The aim of the Code is to obtain even stronger support from managers and employees for our core shared values.

Of course, there are no substitutes for common sense and personal ethics based on respect and responsibility. These values will be your safest guide in finding the right attitude to adopt. However, by expressing the Group's commitment, this Code will help employees to determine their behaviour when faced with actual situations, by referring to clear, precise principles.

Compliance with this Code is the responsibility of all and a priority means of ensuring progress and excellence.

After consulting the Ethics, CSR and Patronage Committee, I have decided to entrust Arnauld Van Eeckhout, the General Counsel of Bouygues, with the position of Group Ethics Officer, as defined in this Code.

Martin Bouygues
Chairman and CEO

PREFACE

The Group Code of Ethics calls on all senior executives and employees to comply with a professional ethic set out in the form of "principles that govern actions" which, under all circumstances and in all countries, must direct senior executive and employee conduct.

These principles that govern actions do not result solely from moral considerations or rules of law, and are not merely reminders of the need to comply with the law. They seek to promote honest and exemplary professional conduct under all circumstances.

Certain issues that are considered to be crucial are set forth in the Compliance Programmes.

However, we can only achieve the goals set out in the Code with thought and a sense of individual responsibility, as the Code cannot reiterate or complement the body of laws, regulations, internal codes and reference manuals that govern the activities of Group companies and employees. Nor can the Code cover all the situations with which senior executives or employees may be confronted within the scope of their activities.

There are numerous situations that are not covered by the laws, regulations and other internal or external standards, which require employee conduct to be governed by respect, fairness and honesty. It is up to each person to examine these situations in light of these principles.

Thoughtfulness, common sense and sound judgment are therefore required of each employee.

The company in which senior executives and employees perform their duties may have laid down specific rules to ensure improved compliance with the laws, regulations and obligations that govern its business activity: this Code does not replace them. However, it is up to each Group company to lay down internal rules that are adapted to its activity and to transpose, to the extent required, the principles defined in the Code of Ethics and the Compliance Programmes.

If this Code is found to be incomplete or imprecise in certain situations, if employees feel uncertainty or doubt as to how to behave when faced with specific situations, they are requested to consult their line management and/or the legal or human resources departments, or the persons in charge of sustainable development.

Employees, the legal and human resources departments, and the persons responsible for sustainable development may also contact and consult the Ethics Officer

of each Business segment[1], or as a last resort the Group Ethics Officer, with respect to any situation or issue concerning ethics. Moreover, Ethics Officers, whether at Business segment or Group level, will bring policies and general issues in the field of ethics before the Ethics, CSR and Patronage Committee of the relevant Board of Directors.

Ethics Officers are also responsible for ensuring that the whistleblowing procedure defined by this Code works properly. They are appointed by the Chairman of each Business segment parent company, after consulting the Ethics, CSR and Patronage Committee of the Board of Directors of the Business segment parent company.

(1) In this Code of Ethics, the term "Business segment" refers to each of the main activities of the Group, which are, as of the date hereof, "Construction" (Bouygues Construction), "Property" (Bouygues Immobilier), "Roads" (Colas), "Media" (TF1) and "Telecoms" (Bouygues Telecom), as well as the parent company (Bouygues SA).

1 COMPLIANCE WITH THE LAW

The Group and its employees[1] must comply with the laws and regulations in every country where they perform their business activities. Employees must avoid activities and behaviour that could involve themselves, other employees, their company or the Group in an unlawful activity.

While we cannot ask everyone to be a specialist in the legislation that applies to their professional activity, individual employees need to acquire sufficient knowledge of the rules of law that are applicable to their activities, regardless of whether the activities are performed in France or abroad.

This basic knowledge will allow them to determine when it is necessary for them to seek counsel from line management, the legal and human resources departments, and possibly from the Group's external counsels.

Strict compliance with the anti-corruption, competition and embargo laws as well as stock market regulations is of utmost importance. The same is true for laws governing respect for human rights and fundamental freedoms, labour and employment, health and safety, personal data protection, and protection of the environment, which require particular vigilance.

(1) In this Code of Ethics, the term "employee" means all senior executives and employees of Bouygues group companies, i.e. all companies controlled directly or indirectly by Bouygues SA pursuant to the combined provisions of Articles L. 233-3 and L. 233-16 of the French Commercial Code.

2 RESPECT FOR PERSONS

Human resources management, the coordination of Group employees and relations between employees are based on the principles of mutual trust and respect, as well as treating others with dignity.

The Group Human Resources Charter is the reference that guides individual employees in their daily work.

The Group seeks to apply a fair policy of human resources that complies with the law. The Group will refrain from, in particular, all discrimination on unlawful grounds.

All psychological and sexual forms of harassment, coercion and bullying are prohibited.

Compliance must be ensured with the laws that govern the protection of employees' privacy, in particular the laws governing electronic files.

Ensuring and improving the safety of employees in the performance of their duties is an ongoing concern.

The Group also seeks to comply with:

- the principles of the United Nations Universal Declaration of Human Rights;
- the fundamental conventions of the International Labour Organisation (ILO), in particular concerning forced and child labour;
- the principles of the United Nations Global Compact.

3 HIGHER INTERESTS OF THE GROUP

Employees must, under all circumstances, be loyal and be guided by the interests of the company for which they work and by the interests of the Group. The quality of the Group's image and the reputation of its services and products are essential for its development and durability. All employees must refrain from any denigrating behaviour as regards the company that employs them or the Group.

Group employees must pay particular attention to the protection and profitability of the investments made by shareholders of Group companies.

Achieving customer satisfaction is a paramount goal for the Group. Customer loyalty is won and maintained through respect for their rights and a permanent concern to make only commitments that can be honoured.

4 INTRA-GROUP RELATIONS

Where several Group companies are required to have business dealings with each other, they shall, with the same vigilance, show the loyalty that customers, suppliers and external partners deserve. In the interests of the Group, they shall implement all measures that make it possible to avoid disputes. Where a dispute cannot be avoided, a fair solution must be sought, with each party acting in a spirit of conciliation, with transparency and in good faith.

In general, while all employees are required to protect the interests of the company where they perform their business activity, they should also be aware that the higher interests of the Group require everyone to ensure the quality and smooth running of internal relations, regardless of the field concerned: contracts concluded within the normal scope of business, commercial and financial relations, but also and particularly, in the field of human resources, e.g. intra-Group job mobility.

5 CONFLICTS OF INTEREST

Given their duty of loyalty towards the Group, employees shall take care not to perform any other activity, either directly or indirectly, and not to make any statements that would place them in a conflict of interest with the company.

In particular, employees must not seek to hold an interest or invest in a business, whether the business is a Group customer, supplier or competitor, if this investment is liable to influence their behaviour in the performance of their duties within the Group.

All employees shall obtain written authorisation from their company senior executive before concluding any transaction with a company where the employee or a member of the employee's family is a major investor or key senior executive.

Employees may not accept an assignment or outside work offered by a supplier, customer or competitor that could affect their performances or judgement in the performance of their duties in the Group.

All employees must inform their line management of any outside assignments and employment of a professional nature and, in general, of any conflict of interest.

Individual common sense and personal conscience can ensure that conflicts of interest are avoided.

6 COMMUNICATIONS AND INFORMATION – FAIRNESS TO SHAREHOLDERS

The Group strives for transparency and reliability in its communications. The aim is to enable Group partners and employees to be accurately informed of Group activities.

The Group seeks to provide reliable and quality information, particularly to its shareholders and financial markets.

Proper Group management requires individual employees, regardless of grade, to take the utmost care with respect to the quality and accuracy of the information they circulate within the Group.

Employees must not disclose the confidential information they hold on account of their duties or simply as a result of belonging to the Group, to parties outside the Group. Employees shall not disclose such confidential information to other Group employees who do not have authorisation to access it. Particular vigilance is required with respect to information on financial results, projections and other financial data, acquisitions and disposals, new products, know-how and techniques, commercial offers and information on human resources. This duty to ensure confidentiality continues even after employees leave the Group.

The prohibition on disclosure encompasses, in particular, certain information and communications initiatives: relations with the media, investors, financial analysts and public and regulatory authorities are the sole responsibility of specific senior executives and specialised departments, such as the communications and finance departments, and departments charged with regulatory affairs. All information, whether confidential or not, and communications initiatives, cannot be disclosed or undertaken by a senior executive, employee or department that has not been given this responsibility.

The high profile that accompanies certain positions in the Group requires particular attention to these duties of discretion and restraint.

7 PROTECTION OF ASSETS

Everyone is responsible for the safeguard of Group assets. These are not only the movable property, real property and intangible assets recognised and defined by the law, but also include the ideas and know-how generated by Group employees. Lists of customers and sub-contractors or suppliers, information on markets, technical and commercial practices, commercial offers and technical studies, and all data and information to which employees have access in the performance of their duties are also part of the Group's assets. These assets are protected and employees remain bound to their duty to protect them even after leaving the Group.

No Group funds or property may be used for unlawful purposes or for purposes that are not connected to Group activities. Therefore, company facilities, equipment, funds, services, and, in general, company assets, must not be used for personal purposes. Employees shall not use any Group assets whatsoever for personal purposes, or place such assets at the disposal of a third party for use for the benefit of any party other than the Group. Any use of the Group's assets in breach of these principles is fraudulent and, therefore, strictly forbidden.

In particular, the communications systems and intranet networks are Group property and should be used for professional purposes. Use for personal purposes is only authorised within reasonable limits if needed to achieve an optimum work-life balance and if really necessary. Using these systems and networks for unlawful purposes, in particular to send defamatory and discriminatory messages of a racist, sexual or insulting nature, is prohibited.

Employees are also prohibited from making illegal copies of the software products used by the Group and from using said software in an unauthorised way.

The confidentiality of all the documents and information that comprise the intellectual, industrial and artistic property and know-how developed directly or indirectly by the Group must be maintained by employees having access to it. Employees with access to such confidential information must refrain from disclosing it to the public and from using it for any purpose other than that authorised by the company. The Group IT Charter covers and develops some of these principles.

8 FINANCIAL TRANSACTIONS – ACCOUNTING

The operations and transactions carried out by the Group must be recorded in an accurate and fair manner in each company's accounts, in accordance with applicable regulations and internal procedures.

In particular, all employees who make accounting entries must show accuracy and honesty, and ensure that each entry is backed up with supporting documents.

All transfers of funds require particular vigilance, in particular regarding the identity of the beneficiary and the reason for the transfer.

The disclosure of financial information and stock market transactions performed by employees involving securities of listed Group companies, whether as part of their duties or for personal purposes, must comply with the laws and regulations that govern financial activities.

The disclosure of inaccurate information and the circulation and use of inside information, as well as share price manipulation, are criminal offences.

It is, in particular, the responsibility of each employee to ensure the confidentiality of all non-public information that could influence the Bouygues share price, or listed securities of any other Group company, until the publication of such information by the authorised persons. Employees shall

also refrain from dealing in Bouygues shares or any other listed securities issued by a Group company, for as long as such information has not been made public. Use of such information directly or indirectly for personal gain or to enable a third party to carry out a stock market transaction is prohibited.

Employees who have doubts or questions, in particular holders of inside information, may consult the Ethics Officer to ensure that they are complying with the ethics and the rules in force governing transactions involving listed securities issued by a Group company and the exercise of stock options.

9 INTERNAL CONTROL

Promoting good ethical conduct across the Group, fighting corruption and fraud and complying with competition law and embargo rules are three of the major themes developed in the Internal Control and Risk Management Reference Manual of the Bouygues group. Ongoing supervision of the application of internal control principles in the field of ethics is carried out by the Business segments and their subsidiaries by implementing the self-assessments set out in the Internal Control Reference Manual.

During regular or specific audit assignments, the internal audit departments of the Group and Business segments also check that the Group's operations are carried out in compliance with the principles of this Code of Ethics and the Group Internal Control Reference Manual. All employees must cooperate with members of the audit departments in a transparent and honest manner, so that any significant deficiency or weakness can be identified and corrected.

Any hindrance to the smooth running of internal audit assignments, as well as any concealment of information or wilful communication of inaccurate information constitute serious breaches of this Code of Ethics.

Employees are required to cooperate in the same way with statutory auditors as part of their assignments.

10 QUALITY

Quality is one of the Group's strategic concerns.

Bouygues group companies have an obligation to treat their customers honestly and fairly. They are convinced that customer satisfaction is key to the Group's long-term future. Group employees and companies give priority to high-quality contact and ensure that product and service quality is constantly improved, paying attention to health and safety in the use of the products offered.

The technologies and processes that are used take into account requirements concerning quality, safety, the environment, and the contractual and regulatory framework.

These requirements are also taken into account through the choice of suppliers and sub-contractors.

The quality-safety-environment certification of our management systems

by an independent organisation increases the confidence of our customers in our capacity to fulfil our commitments.

Employees must contribute to the continuous improvement of internal risk management systems and facilitate the identification of the primary causes of malfunctions.

11 SUSTAINABLE DEVELOPMENT

Sustainable development is included in the strategy of the Group's Business segments. In keeping with its culture and values, the Group undertakes to serve its customers, while assuming social and environmental responsibility.

By applying the principle of continuous improvement and on the basis of concrete actions, Group entities must take into account, in their strategy and processes, the preservation of the environment and natural resources, improvement of living conditions, the sharing of experiences, the use of the best technologies and dialogue with and the involvement of stakeholders in the decisions that concern them.

By adhering to the United Nations Global Compact, the Group shows its commitment to a constant quest for innovative solutions in the field of human rights, labour standards, the environment and anti-corruption. This active approach is central to the Group's culture and values and is implemented in partnership with civil society and other organisations.

12 RESPECT FOR THE ENVIRONMENT

The Group aims to reach the best standards in the field of environmental protection. Employees must make every effort to maintain a safe working environment that protects health. It is also the responsibility of individual employees to prevent or minimise the impacts of their activity on the environment. In particular, the protection of nature, the preservation of biodiversity and eco-systems, the depletion of natural resources and the management of waste and toxic substances are concerns that are common to all Group employees.

13 CHARITABLE CONTRIBUTIONS – PATRONAGE

Charitable contributions and patronage initiatives are authorised if they effectively serve a cause of general interest and contribute to community action initiatives as defined by the Group or its entities. They must receive prior, written approval from the senior executive of the company concerned and must be duly recorded in the accounts.

14 POLITICAL ACTIVITY

The Group respects the commitments of its employees who, as citizens, participate in public life.

In 2017, the Group introduced a system that seeks to eliminate any disadvantage to those who stand for election or exercise a political mandate.

However, the Group seeks to maintain a neutral political stance.

Employees must therefore exercise their freedom of opinion and political activity outside the scope of their employment contract, at their expense and on an exclusively personal basis. No Group asset shall be used for political activities. All employees must refrain from involving the Group and any of its entities in such activities, from a moral standpoint, and are notably prohibited from disclosing their ties with the Group.

The financing of political parties or the activities of elected representatives or candidates by a company is strictly prohibited in France.

In other countries, these contributions are authorised and/or subject to legislation. The general policy of the Group is not to contribute directly or indirectly to the financing of political parties or politicians. If, in a given country, it appears that a company's conduct in society cannot differ from generally accepted practices, all contributions will comply with local legislation, be recorded in the accounts and be subject to the prior written agreement of the senior executive of the contributing company. In any event, such contributions will be limited to the most reasonable amounts contributed in the country concerned and will not seek to promote a specific interest.

Any employee who participates in the decisions of a State, public authority or local government within the scope of their political activities must pay very careful attention to the risk of potential conflicts of interest and refrain from taking part in decisions that concern the Group or one of its entities.

15 COMMERCIAL ACTION – RELATIONS WITH CUSTOMERS AND SUPPLIERS

Group companies must treat all their customers and suppliers with honesty and fairness, regardless of their size and condition.

The Group's commercial action, in France and abroad, will be conducted in compliance with the framework laid down in each country, which employees must observe and be aware of. In particular, Group companies shall comply with the specific rules that govern public procurement contracts, regardless of the country in which they conduct their business activities.

Group companies can only draw benefit from fair and open competition. Group employees and companies shall carry out all commercial action and purchasing by following the principle of fair competition, and by refraining from collusive practices or behaviour that could constitute anticompetitive practices, in particular within the scope of public tenders or contracts concluded with States or local government.

As competition law is complex and subject to change, and as administrative, criminal and civil sanctions may be applied, employees shall consult with the legal departments in the event of a doubt or question.

Employees must undertake not to offer or grant favours or benefits, whether pecuniary or otherwise, to third parties. In particular, the promising or giving of gifts or free services are not permitted, unless as a matter

of courtesy or customary hospitality, or unless the gifts are symbolic or minimal. In general, commercial dealings must comply with the legislation applicable to the activity concerned and remain within the limits of the most reasonable customary practices for the profession or country where they are implemented.

The support given by agents, consultants or intermediaries in the area of commercial dealings may be required in the sectors where Group presence is reduced or due to their technical skills. Calling on these intermediaries is only justified within this scope and only if the services provided are genuine, lawful and necessary. Their remuneration must be in keeping with the services and the payment compliant with their contract, which must be concluded in compliance with internal procedures.

The senior executives of the companies concerned must ensure that they supervise this local support and monitor the services effectively provided by these intermediaries, in strict compliance with local rules.

Employees must not agree to receive, either directly or indirectly, any payment, gift, loan, entertainment or benefit from anyone who does business with the Group; only customary courtesy or hospitality, business meals and other events that correspond to the most reasonable customary practices in the country or profession are acceptable. Gifts, other than pecuniary gifts, are acceptable if their value is low and if such a practice complies with customary practices. Employees must ask themselves whether such a gift or benefit is lawful, liable to affect how they act within the Group and whether the giver will think that employees have compromised themselves. The line management must be informed of any canvassing or offer of specific benefits to employees.

Finally, fraud – that is to say any act or omission with intent to deceive (falsification, dissimulation, lying, etc.) – both internally and externally, is unacceptable and breaches the Group's values. All employees must, under all circumstances, observe the highest standards of honesty and integrity in their relations with co-contractors and customers, in particular as regards the nature, quality, quantity, and the composition of products and services offered.

16 CORRUPTION

Acts of corruption breach the Group's ethical principles and values.

The negotiation and performance of contracts must, under no circumstances, give rise to conduct or actions that could constitute active or passive corruption towards or on behalf of public or private entities, or complicity in influence peddling or favouritism. It should be noted that offences committed by intermediaries, commercial agents or consultants could result in the person having hired them being liable to severe sanctions in the same way as a direct perpetrator would.

In accordance with the OECD Convention of 17 December 1997 on Combating Bribery, the corruption of foreign public officials, in all forms, is prohibited.

17 COMPLIANCE PROGRAMMES/ DUTY OF VIGILANCE

Certain principles that govern actions in areas that are considered to be crucial are developed in the Compliance Programmes. The Bouygues Board of Directors has approved five Compliance Programmes (Anti-corruption, Competition, Conflicts of Interest, Financial Information and Securities Trading, and Embargoes and Export Restrictions) and reserves its right, if necessary, to approve other programmes.

These Compliance Programmes, that supplement this Code of Ethics, set out and explain, for each of the subjects covered, the main rules applicable, the Group's position and the main principles with which senior executives and employees must scrupulously comply. In addition, they set out the best conduct to adopt and precautions to take in each of the areas concerned to prevent, in all circumstances, anyone or the company from being put in a difficult situation.

In accordance with the law of 27 March 2017, Bouygues draws up a Group vigilance plan that sets out the reasonable vigilance measures to be taken to identify risk and prevent serious violations of human rights and fundamental freedoms, the health and safety of people and the environment caused by the activities of the Group or the sub-contractors or suppliers with which it maintains an established business relationship.

18 IMPLEMENTATION OF THE CODE OF ETHICS, COMPLIANCE PROGRAMMES AND VIGILANCE PLAN

It is the responsibility of each Business segment to implement this Code of Ethics and the Compliance Programmes, and to complete them if necessary in accordance with the specificities of its activities.

The Code of Ethics and Compliance Programmes can be accessed on the intranet. All senior executives and employees who join one of the Group entities may also be provided with a paper copy of the Code of Ethics.

All employees are required to comply with and apply the rules contained in this Code of Ethics, the Compliance Programmes and vigilance plan, according to their duties and responsibilities. To this end, employees must actively participate in their implementation and be vigilant with regard not only to themselves, but also to their circle of contacts, their teams and the persons placed under their responsibility.

19 WHISTLEBLOWING

When confronted with an ethical problem, employees must inform their direct or indirect line manager or the senior executive of the company where they perform their duties, allowing sufficient time for said line managers or senior executives to give relevant advice or to take an appropriate decision.

It is the responsibility of the line managers and senior executives of a company to assist employees in

resolving the difficulties with which they may be confronted. When in doubt, the legal or human resources departments, as well as possibly external counsels, should be consulted.

Employees who, disinterestedly and in good faith, report a breach of the rules laid down in this Code shall not be sanctioned.

Employees may also use the Group whistleblowing facility to report, disinterestedly and in good faith, facts or events they have personally witnessed or have first-hand knowledge of, which fall within the scope of the Group whistleblowing facility. The Group whistleblowing facility is governed by the following rules:

Scope of the Group whistleblowing facility

The scope of the whistleblowing facility was extended in 2017. It includes:

- any crime or offence;
- any serious and blatant violation of a law or regulation, an international treaty or convention ratified or approved by France (including a unilateral action taken by an international organisation on the basis of an international treaty or convention ratified or approved by France);
- serious threat or harm to the public interest.

It covers, in particular, the following areas:

- corruption and influence peddling (especially any behaviour or situation that breaches the rules set out in the Anti-corruption Compliance Programme);
- accounting irregularities;
- stock market irregularities;
- violation of competition and embargo rules and standards;
- existence or materialisation of risks related to serious violations of human rights and fundamental freedoms, the health and safety of people and the environment, caused by the activities of the Group or the sub-contractors and suppliers with which it maintains an established business relationship.

Regardless of their form or media, facts, information or documents covered by national defence secrecy, doctor/patient confidentiality or lawyer/client privilege are specifically excluded from the Group's whistleblowing facility. However, a breach of these secrecy or confidentiality rules through the whistleblowing facility may exceptionally be envisaged provided that such disclosure is necessary and commensurate with safeguarding the interests in question, that it is done through the whistleblowing facility and that the person raising the whistleblowing alarm meets all the requisite criteria for definition as a whistleblower.

The persons concerned by the Group whistleblowing facility

Any employee of a Group company may use the Group's whistleblowing facility. It is also open to external or occasional employees (e.g. temporary workers, interns, employees of a sub-contractor or service provider) other than for reporting conduct or situations that contravene the Anti-

corruption Compliance Programme[1], which is restricted to employees of Group companies.

Any employee may be the subject of a whistleblowing alert. However, certain employees are more likely to be targeted in the following areas:

- Corruption:
  Senior executives, managers and employees from the purchasing, projects, works, general services, IT, sales and marketing departments.
- Accounting irregularities:
  Senior executives, managers and employees from the consolidation, accounting, cash management and finance departments.
- Stock market irregularities:
  Senior executives, managers and employees from the cash management and finance departments and, in general, all employees who may hold inside information.
- Competition irregularities:
  Senior executives, managers and employees of the purchasing, sales, works or projects departments.
- Human rights and fundamental freedoms:
  Site managers, particularly in the international markets, human resources departments of operational units, particularly in the international markets, IT department employees and managers.

Initiating an alert via the Group whistleblowing facility

Use of the whistleblowing facility is optional. The facility should only be used in compliance with the applicable laws and regulations and provided that the whistleblower is acting disinterestedly and in good faith and has personally witnessed or has first-hand knowledge of the events or facts in question.

The fact that an employee refrains from using the whistleblowing facility may not lead to any consequences for the employee concerned.

A whistleblower who makes proper use of the facility will not be liable to disciplinary action or discriminatory measures of any kind, even if the facts are subsequently found to be inaccurate or not proven. However, abuse of the facility will render the whistleblower liable to disciplinary action and, potentially, to legal proceedings.

Recipient(s) of the whistleblowing alert

Data and information must be provided by the whistleblower to the Business segment Ethics Officer[2] concerned, who shall, to that end, be subject to an increased confidentiality obligation.

However, as an exception, an employee faced with a situation that he or she believes to go beyond the scope of the Business segment may refer to the Group Ethics Officer[3], who is also subject to an increased confidentiality obligation.

(1) The Anti-Corruption Compliance Programme constitutes the code of conduct referred to in Article 17 of law No. 2016-1691 of 9 December 2016, known as the "Sapin 2" law.
(2) The designated recipient ("référent") referred to in the applicable regulations.
(3) In this case, the designated recipient ("référent") referred to in the applicable regulations.

Receipt and processing of whistleblowing alerts

The procedure for the receipt and processing of whistleblower alerts is set out in Appendix 1 to this Code of Ethics. It has been drawn up in consultation with Bouygues' registered trade unions.

The rights of persons implicated in a Group whistleblowing alert

All persons implicated in a whistleblowing alert will be informed by its recipient as soon as their personal data has been logged, electronically or otherwise. The person will be able to access the data and request the correction or deletion thereof if the data is incorrect, unclear or obsolete.

Where protective measures are required, in particular to prevent the destruction of evidence concerning the whistleblowing alert, the person implicated in the whistleblowing alert will only be informed once these measures have been taken.

The following information, in particular, will be provided to all persons implicated in a whistleblowing alert:

- a copy of these rules, which govern the Group whistleblowing facility, and a copy of the laws on whistleblowing;
- the allegations made against them;
- a list of the recipients of the whistleblowing alert;
- the terms and conditions for exercising their access and rectification rights.

Persons implicated in a whistleblowing alert may under no circumstances obtain disclosure of the identity of the whistleblower.

CONTACT

Group Ethics Officer

Arnauld Van Eeckhout
General Counsel, Bouygues
Email: avet@bouygues.com

APPENDIX

WHISTLEBLOWING FACILITY: PROCEDURE AND RULES PERTAINING TO THE RECEIPT AND PROCESSING OF WHISTLEBLOWING ALERTS

1 RAISING A WHISTLEBLOWING ALERT: REMINDER

To raise a whistleblowing alert under the whistleblowing facility, you must do so disinterestedly and in good faith. You must have personally witnessed or have first-hand knowledge of the facts or events you are reporting.

2 WHERE TO SEND A WHISTLEBLOWING ALERT

Whistleblowing alerts must be sent to the Ethics Officer of the relevant Business segment, who is the designated recipient ("*référent désigné*") under the applicable regulations.

However, if you believe that the situation goes beyond the scope of the Business segment, you may exceptionally send your whistleblowing alert to the Group Ethics Officer instead of the Business segment Ethics Officer.

3 HOW TO RAISE A WHISTLEBLOWING ALERT

Any whistleblowing alert sent as part of this whistleblowing facility must meet the following criteria:

- **Method:** whistleblowing alerts should be sent by post, secure e-mail (encrypted) or via the dedicated platform[1], for the sole attention of the recipient of the whistleblowing alert (see table on page 22).

  However, should you raise a whistleblowing alert by telephone or during a private conversation with the designated recipient of the whistleblowing alert, such an alert shall, where practicable, be confirmed in writing.

  For reasons of confidentiality, all whistleblowing alerts reported by e-mail must comply with the instructions in the table on page 22.
- **Subject heading:** the subject heading of the letter or e-mail must clearly indicate that a whistleblowing alert is being raised under the whistleblowing facility.
- **Identity of whistleblower:** your whistleblowing alert must provide details of your identity, as well as the contact details permitting an exchange between you and the designated recipient of the whistleblowing alert (first name, last name, employer, position, home address, e-mail address, phone numbers, etc.).

4 DESCRIPTION OF THE FACTS OR EVENTS

You must provide a clear, impartial description of the facts and information you are reporting. The wording used must make it clear that the events or facts reported are presumptions.

(1) The dedicated platform will be available online in 2018 at https//alertegroupe.bouygues.com.

The designated recipient of the whistleblowing alert will only consider information directly related to the areas covered by the whistleblowing facility and which is strictly necessary in order to investigate the allegations. Any information that does not meet these requirements will be destroyed.

Should you deem it appropriate to implicate one or more individuals in your whistleblowing alert, you should follow the procedure set out below in order to protect the identity of the person or persons you are implicating:

- if you are raising your whistleblowing alert by e-mail, you should only send it by secure e-mail or via the dedicated platform[1];
- you must never reveal the fact that you have raised a whistleblowing alert (except as part of the processing of a whistleblowing alert), and more specifically its contents or the persons implicated.

5 PROOF – DOCUMENTATION

You should provide any documents or information in your possession you have to support your allegations, whatever the format or medium.

You may simply list them in your initial letter or e-mail and then provide them promptly to the designated recipient of the whistleblowing alert.

Any information given in the whistleblowing alert that does not fall within the scope of the whistleblowing facility will be destroyed or archived immediately by the designated recipient of the whistleblowing alert, unless the company's vital interests or the physical or moral integrity of its employees are at risk.

6 ACKNOWLEDGEMENT OF RECEIPT

As soon as the whistleblowing alert has been received, the designated recipient of the whistleblowing alert will reply by recorded delivery letter, secure e-mail or via the dedicated platform, with the following information:

- acknowledgement of receipt of your whistleblowing alert;
- if applicable, any other information required for your whistleblowing alert to be processed;
- the anticipated duration of the processing of your whistleblowing alert;
- how you will be advised (letter, secure e-mail or via the dedicated platform) of the action(s) taken as a result of your whistleblowing alert. This information will normally be given to you before the end of the period referred to above.

You will be informed promptly should the designated recipient of the whistleblowing alert deem that the prerequisites for the processing of your whistleblowing alert are not met.

7 CONFIDENTIALITY GUARANTEE

The designated recipient of the whistleblowing alert will take all necessary measures to protect the security and confidentiality of any information provided, not only when the alert is received but also during the investigations and as long as such information is retained.

(1) The dedicated platform will be available online in 2018 at https//alertegroupe.bouygues.com.

More specifically, data can only be accessed via an individual user login and password, which are changed regularly, or by any other means of authentication. Access to data is recorded and controlled. The designated recipient of the whistleblowing alert is bound by a heightened contractual confidentiality undertaking.

Whistleblowing alerts are received and processed in a way that guarantees the strict confidentiality of:

- the whistleblower's identity;
- the identity of the persons implicated in the whistleblowing alert;
- information provided in the whistleblowing alert.

Any information that might permit the identification of the whistleblower may not be disclosed, other than to the judicial authorities, without the whistleblower's prior consent.

Any information that might permit the identification of the persons implicated in a whistleblowing alert may not be disclosed, other than to the judicial authorities, until the merits of the allegation have been established.

Consequently, the following procedure will apply:

- whistleblowing alerts raised by e-mail must only be sent by secure e-mail or via the dedicated platform[1], which can only be accessed by the designated recipient of the whistleblowing alert. The designated recipient of the whistleblowing alert is notified via e-mail that a whistleblowing alert has been raised;
- acknowledgement of receipt will be sent by recorded delivery letter, secure e-mail or via the dedicated platform[1];
- when processing a whistleblowing alert, the designated recipient of the whistleblowing alert shall not mention the name of the person(s) implicated, except, as appropriate: (i) to the direct or indirect line manager of the implicated person(s), where necessary for internal investigation purposes, in accordance with applicable legal provisions, (ii) to the Group Ethics Officer or (iii) to the judicial authorities. Nor will the designated recipient of the whistleblowing alert disclose any information that might permit the identification of the person(s) implicated in a whistleblowing alert. The direct or indirect line manager of the implicated person(s) and the Group Ethics Officer are bound by the same strict confidentiality undertaking as the designated recipient of the whistleblowing alert.

8 RIGHTS OF PERSONS IMPLICATED IN A WHISTLEBLOWING ALERT — DATA PROTECTION

If you are implicated in a whistleblowing alert, you will be informed by the designated recipient of the whistleblowing alert as soon as your personal data has been logged, electronically or otherwise. You have the right to access the data, ask for it to be rectified or deleted if it is incorrect, unclear or obsolete. You should exercise this right by contacting the

(1) The dedicated platform will be available online in 2018 at https//alertegroupe.bouygues.com.

designated recipient of the whistleblowing alert in your Business segment, at the address given in the table on page 22.

When protective measures are necessary, particularly to avoid the destruction of evidence about the whistleblowing alert raised, you will only be informed once those measures have been taken.

The designated recipient of the whistleblowing alert will inform you of the allegations made against you.

You may obtain the following information at your request:

- a copy of these rules governing the Group's whistleblowing facility;
- a copy of the legal provisions on whistleblowing as applicable under French law.

You will under no circumstances be informed of the whistleblower's identity.

9 HOW A WHISTLEBLOWING ALERT IS PROCESSED

As part of a preliminary review, the Ethics Officer will first make sure that the whistleblower has acted within the scope of the whistleblowing facility and in accordance with the applicable regulations. If the Ethics Officer deems this is not the case, you will be informed promptly. The designated recipient of the whistleblowing alert may ask you to provide additional information before the investigation of the merits of the whistleblowing alert is initiated. During the processing of the whistleblowing alert, the wording used should make it clear that the events or facts being reported are presumptions.

When processing the whistleblowing alert, the designated recipient of the whistleblowing alert may make any enquiries deemed appropriate to assess the merits of the alert. The designated recipient of the whistleblowing alert may involve the implicated person's/persons' line managers (provided they are not implicated) or any employee whose involvement is believed necessary as part of the processing of the whistleblowing alert, always in the strictest of confidence.

The designated recipient of the whistleblowing alert may also inform and obtain the opinion of the Group Ethics Officer or the competent Ethics Committee. The designated recipient of the whistleblowing alert may also ask the whistleblower for further information.

As part of the investigations, any outside service provider may be called upon, and shall act in the strictest confidence.

If the designated recipient of the whistleblowing alert believes that the investigation process will take longer than initially expected, the whistleblower shall be informed and be provided with the reasons for the extra time needed, if this is deemed appropriate, as well as with the ongoing status of the investigations.

The receipt and processing of the whistleblowing alert will always be conducted so as to allow all implicated parties to argument and respond to any allegations made as part of the alert or investigations (the adversarial process principle) and in accordance with the provisions of labour law.

Whistleblowers shall never receive any compensation or gratuity for raising a whistleblowing alert; it is a strictly disinterested process.

10 ACTION TAKEN FOLLOWING THE WHISTLEBLOWING ALERT – CLOSE OF PROCEDURE

Once the investigations are complete, a decision will be made on the action to be taken, which may include disciplinary action against the person(s) who has (have) committed or taken part in the wrongdoing and/or, as the case may be, referral of the matter to the administrative or judicial authorities.

The whistleblower will be informed of the action(s) taken as a result of the whistleblowing alert by letter, secure e-mail or via the dedicated platform. The whistleblower and the persons implicated will also be informed that the whistleblowing procedure has been closed.

If, once the investigations are complete, no disciplinary or legal action is to be taken, the information contained in the whistleblowing alert identifying the whistleblower and the person(s) implicated will be destroyed or archived promptly (and no later than two months after the investigations have ended).

The information will be destroyed regardless of the medium on which it is stored, including electronic data.

11 DISSEMINATION OF THE PROCEDURE

This procedure is an appendix to the Group Code of Ethics. It will be disseminated to employees by all appropriate means:

- wherever possible, a paper copy of the Code of Ethics will be provided to all new employees;
- publication on the websites and intranet sites of Bouygues and the Business segments;
- display on company notice boards.

The procedure must be made available to all employees, including external and occasional workers.

12 REMINDER OF THE LEGAL PROVISIONS

No disciplinary or other action may be taken against an employee who raises a whistleblowing alert disinterestedly and in good faith, provided such an alert falls within the scope of the whistleblowing facility and the procedure is complied with by the whistleblower.

Conversely, anyone who abuses the facility or acts with malicious intent will be liable to disciplinary action and, potentially, legal proceedings. The criminal penalties provided for in Article 226-10 of the French Criminal Code may apply to anyone who knowingly makes a malicious accusation.

13 ENTITY RESPONSIBLE FOR THE WHISTLEBLOWING FACILITY

The entity responsible for the whistleblowing facility is either the relevant Business segment or Bouygues SA[1]. These entities are listed in the table below (see page 22).

(1) When the Group Ethics Officer or Bouygues SA is the recipient of the whistleblowing alert (regardless of the Business segment concerned).

List of Ethics Officers (Group, Business segment)

Business segment	Name	Contact details (France)
Group and/or Bouygues SA	Mr Arnauld Van Eeckhout	E-mail: alerte@bouygues.com Address: 32 avenue Hoche 75378 Paris cedex 08 Tel.: +33 (0)1 44 20 10 18
Bouygues Construction	Mr Jean-Marc Kiviatkowski	E-mail: alerte_ethique@bouygues-construction.com Address: 1 avenue Eugène Freyssinet 78280 Guyancourt Tel.: +33 (0)1 30 60 26 48
Bouygues Immobilier	Mrs Charlotte Lavedrine	E-mail: alerteprofessionnelle@bouygues-immobilier.com Address: 3 boulevard Gallieni 92130 Issy-les-Moulineaux Tel.: +33 (0)1 55 38 26 24
Colas	Mr Ronan Raffray	E-mail: alertethics@colas.com Address: 7 place René Clair 92100 Boulogne-Billancourt Tel.: +33 (0)1 47 61 73 61
TF1	Mr Jean-Michel Counillon	E-mail: alerteprofessionnelle@tf1.fr Address: 1 quai du Point du Jour 92100 Boulogne-Billancourt Tel.: +33 (0)1 41 41 22 67
Bouygues Telecom	Mrs Anne Friant	E-mail: alerte@bouyguestelecom.fr Address: 37-39 rue Boissière 75116 Paris Tel.: +33 (0)1 39 45 33 66

PROVISIONS OF LAW NO. 2016-1691 OF 9 DECEMBER 2016 ("SAPIN 2 LAW") ON WHISTLEBLOWING (LAW OF THE FRENCH REPUBLIC)

Disclaimer: This is a non-official translation of a French law, for information purposes only. The French version of this text as published in the "Journal Officiel de la République Française" (official gazette of the French Republic) is the only legally binding version.

[...]

CHAPTER II: PROTECTION OF WHISTLEBLOWERS

Article 6

A whistleblower is an individual who reveals or reports, disinterestedly and in good faith, a crime or offence, a serious and blatant violation of an international undertaking ratified or approved by France or a unilateral action taken by an international organisation on the basis of such an undertaking, of a law or regulation, or a serious threat or harm to the general interest, of which that individual has first-hand knowledge or has personally witnessed.

Facts, information or documents, regardless of their form or medium, covered by national defence secrecy, doctor/patient confidentiality or client/attorney privilege are specifically excluded from the whistleblowing provisions stipulated in this chapter.

Article 7

Book I, Title II, Chapter II of the Criminal Code is supplemented by Article 122-9 as follows:

"Article 122-9. A person who discloses secret information, within the meaning of and as protected by law, is not criminally liable where such disclosure is necessary and commensurate with safeguarding the interests in question, is done in accordance with the whistleblowing procedures defined by law and provided that such person meets the definition of a whistleblower set out in Article 6 of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation."

Article 8

I. - The whistleblowing alert shall be raised with the whistleblower's direct or indirect line manager or the recipient (*"référent"*) designated by the employer.

If no action is taken by that person (as referred to in the first paragraph of I above) within a reasonable period of time, the whistleblower may then refer it to the judicial authority, administrative authority or appropriate professional body.

As a last resort, if no action is taken by those authorities or bodies (as

referred to in the second paragraph of I above) within 3 months, the whistleblowing alert may be made public.

II. - In the event of serious and imminent danger or the risk of irreversible damage, the whistleblowing alert may be raised directly with the authorities or bodies referred to in the second paragraph of I above. It may be made public.

III. - Appropriate whistleblowing procedures designed for the receipt of whistleblowing alerts raised by employees and external or occasional workers shall be implemented by public or private sector companies with at least fifty employees, state administrations, municipalities with more than 10,000 inhabitants as well as the fiscally independent public inter-municipal cooperation bodies to which such municipalities belong, departments and regions, in accordance with the conditions stipulated by *Conseil d'État* (French Supreme Administrative Court) decree.

IV. - Anyone may refer to the French Commissioner for Human Rights for guidance on where and how to raise a whistleblowing alert.

Article 9

I. - The whistleblowing procedures implemented in accordance with the provisions of Article 8 shall guarantee strict confidentiality of the whistleblower's identity, the identity of the persons implicated in the whistleblowing alert and the information received by all recipients of the alert.

Any information that might permit the identification of the whistleblower may not be disclosed, other than to the judicial authorities, without the whistleblower's prior consent.

Any information that might permit the identification of the persons implicated in a whistleblowing alert may not be disclosed, other than to the judicial authorities, until the merits of the allegation have been established.

II. - The penalty for disclosure of the confidential information referred to in I above is two years' imprisonment and a fine of €30,000.

Article 10

I. - Article L. 1132-3-3 of the French Labour Code is amended as follows:

1° After the first paragraph, the following paragraph is inserted:

"No one may be excluded from a recruitment process or refused access to an internship or vocational training course, and no employee may be subject to disciplinary action, dismissed or subject to direct or indirect discriminatory measures, notably measures relating to remuneration as defined by Article L. 3221-3, profit-sharing or share awards, training, reconversion, assignment, qualification, classification, professional promotion, internal transfer or contract renewal, for having raised a whistleblowing alert in accordance with Articles 6 to 8 of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation";

2° The first sentence of the second paragraph is amended as follows:

"In the event of a legal action pursuant to the first and second paragraphs above, where the person provides

evidence leading to the presumption that the person has, in all good faith, reported or testified to facts constituting an offence or crime, or has raised a whistleblowing alert in accordance with Articles 6 to 8 of law No. 2016-1691 of 9 December 2016, it is the responsibility of the defendant to prove, in light of the facts, that its decision was justified by objective evidence unrelated to the statement or testimony of the claimant."

II. - Article 6 *ter* A of law No. 83-634 of 13 July 1983 on the rights and obligations of civil servants is amended as follows:

1° After the first paragraph, the following paragraph is inserted:

"No civil servant may be subject to disciplinary action or to direct or indirect discriminatory measures for having raised a whistleblowing alert in accordance with Articles 6 to 8 of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation";

2° The first sentence of the penultimate paragraph is amended as follows:

a) The word "three" is replaced by the word "four";

b) The words "or a conflict of interest situation" are replaced by the words "or a conflict of interest situation or a whistleblowing alert raised within the meaning of Article 6 of the aforementioned law No. 2016-1691 of 9 December 2016";

3° The final paragraph is amended as follows:

"A civil servant who reports or testifies to facts relating to a conflict of interest situation or any event liable to lead to disciplinary action, with malicious intent or knowing that at least some of the facts made public or disclosed are false, shall be liable to the penalties provided for in paragraph 1 of Article 226-10 of the French Criminal Code."

Article 11

After Article L. 911-1 of the French Code of Administrative Justice, an Article L. 911-1-1 is inserted as follows:

"Art. L. 911-1-1.-When Article L. 911-1 is applied, the court may order the reinstatement of any person who has been dismissed or whose contract has not been renewed or has been terminated in violation of the provisions of paragraph 2 of Article L. 4122-4 of the French Defence Code, paragraph 2 of Article L. 1132-3-3 of the French Labour Code or paragraph 2 of Article 6 *ter* A of law No. 83-634 of 13 July 1983 on the rights and obligations of civil servants, even where that person was on fixed-term contract with the public entity or private organisation responsible for managing a public service."

Article 12

If the employment contract is terminated as a result of the employee raising a whistleblowing alert within the meaning of Article 6, the employee may refer to the Employment Tribunal *(Conseil des Prud'hommes)* in accordance with the conditions provided for in Book IV, Title V, Chapter V of the first part of the French Labour Code.

Article 13

I. - Any person who in any way impedes the raising of a whistleblowing alert with the persons and

organisations referred to in the first two paragraphs of Article 8.I is liable to one year's imprisonment and a fine of €15,000.

II. - If the whistleblower is sued for defamation, the amount of the civil fine that may be imposed by the court in accordance with the conditions provided for in Articles 177-2 and 212-2 of the French Code of Criminal Procedure shall be increased to €30,000.

Article 14

[Provisions declared anti-constitutional by *Conseil Constitutionnel* (French Constitutional Court) decision No. 2016-741 DC of 8 December 2016].

Article 15

I. - After the first paragraph of Article L. 4122-4 of the French Defence Code, a new paragraph is inserted as follows:

"No military employee may be subject to disciplinary action or to direct or indirect discriminatory measures for having raised a whistleblowing alert in accordance with Articles 6, 7 and 8.I of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation."

II. - Articles L. 1351-1 and L. 5312-4-2 of the French Public Health Code are repealed.

III. - Articles L. 1161-1 and L. 4133-5 of the French Labour Code are repealed.

IV. - Article 1, points 3° and 4° of Article 2 and Article 12 of law No. 2013-316 of 16 April 2013 on the independence of health and environment experts and whistleblower protection are repealed.

V. - Article 25 of law No. 2013-907 of 11 October 2013 on transparency in public life is repealed.

VI. - [Provisions declared anti-constitutional by *Conseil Constitutionnel* (French Constitutional Court) decision No. 2016-741 DC of 8 December 2016.]

[...]

Link to Sapin 2 law:
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528&dateTexte=&categorieLien=id

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – CNIL (FRENCH DATA PROTECTION AUTHORITY)

Deliberation No. 2017-191 of 22 June 2017 amending deliberation No. 2005-305 of 8 December 2005 on the single authorisation for automatic processing of personal data obtained through a corporate whistleblowing facility (AU-004)

Disclaimer: This is a non-official translation of a French law, for information purposes only. The French version of this text as published in the "Journal Officiel de la République Française" (official gazette of the French Republic) is the only legally binding version.

NOR : CNIL1721434X

The Cnil (French Data Protection Authority)

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Having regard to law No. 78-17 of 6 January 1978 on data protection, files and privacy as amended by law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data, and in particular its Articles 25-I-3°, 25-I-4° and 25-II;

Having regard to law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation;

Having regard to decree No. 2017-564 of 19 April 2017 on whistleblowing procedures in public or private companies and state administrations;

Having regard to deliberation No. 2005-305 of 8 December 2005 on the single authorisation for the automatic processing of personal data obtained through whistleblowing facilities;

Having regard to deliberation No. 2010-369 of 14 October 2010 amending single authorisation No. 2005-305 of 8 December 2005 No. AU-004;

Having regard to deliberation No. 2014-042 of 30 January 2014 amending single authorisation No. 2010-369 of 14 October 2010 No. AU-004;

Having regard to the whistleblowing guidelines adopted by the Commission on 10 November 2005, appended to this decision;

Having heard the report of Mrs Marie-France Mazars, member of the Commission, and the findings of Mrs Nacima Belkacem, Government representative to the Commission,

Issues the following opinion:

A whistleblowing facility is a system set up by public or private organisations for their employees and external and occasional workers, in addition to the normal channels for reporting incidents or problems, to encourage them to report any behaviour they have personally witnessed or have first-hand knowledge of and which they deem to be in violation of the applicable rules, and to organise the conduct of investigations into whistleblowing alerts so received within the relevant organisation.

Notes that whistleblowing facilities implemented in the workplace may involve the automatic processing of personal data that could lead to depriving individuals of the benefits of their employment contract in the absence of legislative or regulatory protection, and may also contain data relating to offences.

Consequently, such systems constitute processing of data covered by Article 25-I 3° and Article 25-I-4° of the law of 6 January 1978 as amended and must, accordingly be authorised by the Cnil.

Pursuant to Article 25-II of the law of 6 January 1978 as amended, the Cnil may adopt a single authorisation for the processing of personal data for the same end purposes, involving identical categories of data and identical categories of recipients.

The data controller responsible for a whistleblowing facility shall, in accordance with the provisions of this decision, send the Cnil a statement of compliance with the single authorisation.

Decides that data controllers who send the Cnil a statement of compliance with the conditions for processing personal data set out in this single decision shall be authorised to undertake such processing.

Art. 1 – Purpose of data processing

Automatic processing of personal data by public or private organisations for the purpose of the notification and processing of the whistleblowing alerts raised by an individual under a whistleblowing facility may be the subject of a statement of compliance with this single authorisation when such an alert relates to:

- a crime or offence;
- a serious and blatant violation of an international undertaking duly ratified or approved by France;
- a serious and blatant violation of a unilateral action taken by an international organisation on the basis of an international undertaking duly ratified by France;
- a serious and blatant violation of a law or regulation;
- or a serious threat or harm to the public interest, of which the whistleblower has first-hand knowledge or has personally witnessed.

This single authorisation also covers automatic processing of personal data implemented by organisations for purposes of the receipt of whistleblowing alerts obtained and emanating from its employees under a whistleblowing facility when it relates to the obligations defined in the European regulations and in the French Monetary and Financial Code or the General Regulation of the *Autorité des Marchés Financiers* (French Securities Regulator), which are supervised by the *Autorité des Marchés Financiers* or

the *Autorité de Contrôle Prudentiel et de Résolution*.

It also covers automatic processing of personal data obtained by an organisation from its employees under a whistleblowing facility when it relates to the existence of behaviour or situations contrary to the company's code of conduct involving corruption or influence peddling.

This is the case so long as the implementation of such data processing is made pursuant to a legal requirement or falls within the legitimate interests of the data controller.

However, a whistleblowing alert must not include information protected by national defence secrecy, patient/doctor confidentiality or client/attorney privilege.

Art. 2 – Processing the identity of the whistleblower and the person implicated

The whistleblower must provide an identity that shall be kept strictly confidential by the organisation responsible for the management of whistleblowing alerts.

The organisation shall not encourage potential whistleblowers to raise whistleblowing alerts anonymously.

Exceptionally, a whistleblowing alert raised by a person who wishes to remain anonymous may be processed provided that:

1. the seriousness of the facts or events is demonstrated and the factual information is sufficiently detailed;

2. special precautions are taken during processing, such as a preliminary review by the designated recipient as to whether or not the whistleblowing alert should be taken further.

Any information that might permit the identification of the whistleblower may not be disclosed, other than to the judicial authorities, without the whistleblower's prior consent.

Any information that might permit the identification of the person implicated may not be disclosed, other than to the judicial authorities, until the merits of the allegation have been established.

Art. 3 – Categories of personal data that may be processed

Only the following categories of data may be processed:

- whistleblower's identity, functions and contact details;
- identity, functions and contact details of the persons implicated in the whistleblowing alert;
- identity, functions and contact details of the persons involved in the receipt or processing of the whistleblowing alert; the facts or events reported;
- information obtained during investigation of the facts or events reported; investigation report; action(s) taken.

The facts and events processed are strictly limited to those covered by the whistleblowing facility. The data may only be taken into consideration if it is expressed disinterestedly, relates directly to the scope of the whistleblowing facility and is strictly necessary in order to investigate the allegations. The wording used shall make it clear that the events or facts being reported are presumptions.

Art. 4 – Recipients of personal data

Unless otherwise provided by laws and regulations, whistleblowing alerts shall be sent to the whistleblower's direct or indirect line manager, employer or employer's designated recipient of the whistleblowing alert. Such recipients shall only receive all or part of the data referred to in Article 4 to the extent required for them to fulfil their duties.

The data may be transferred to persons with specific responsibility for managing the whistleblowing facility in the group of companies to which the organisation belongs, where this is necessary for the sole purpose of verifying or processing the whistleblowing alert.

If the organisation uses a designated recipient of the whistleblowing alert or a service provider to receive or process the whistleblowing alerts, the persons with specific responsibility for such function within that organisation shall only have access to the data referred to in Article 3 to the extent required to fulfil their respective duties. The designated recipient of the whistleblowing alert or service provider appointed to manage all or part of the whistleblowing facility shall contractually undertake not to use the data obtained for unauthorised purposes, to keep it strictly confidential, to comply with the limited data retention period and to destroy or return all the paper or electronic media containing the personal data once its aforementioned duties have been completed.

In all cases, the persons in charge of the receipt and processing of the whistleblowing alerts shall be limited in number, shall receive specific training and shall be subject to a heightened duty of confidentiality.

Art. 5 – Transfer of personal data outside the European Union

This Article shall apply in cases when the data transfers referred to in Article 4 are to be made to a legal entity in a country that is not a member of the European Union and does not provide adequate protection within the meaning of Article 68 of the law of 6 January 1978 as amended.

In such cases, the personal data shall be transferred strictly in accordance with the specific provisions of the law of 6 January 1978 as amended on international transfers of data, and in particular Article 69, paragraph 8.

These provisions shall be deemed to have been met if the legal entity in which the recipient of the data works is a member of the Privacy Shield, provided that such a US company has expressly opted to include Human Resources data within the scope of this framework.

These provisions shall also be deemed to have been met if the recipient has entered into contractual transfer agreement based on the standard contractual clauses issued by the European Commission in its decisions of 15 June 2001 and 27 December 2004, or if the group to which the relevant entities belong have adopted internal rules that have been expressly recognised by the Cnil beforehand as guaranteeing a sufficient level of protection of privacy and fundamental human rights. If these conditions are met and the processing giving rise to

the transfer also complies with all the other provisions of this deliberation, this deliberation shall also constitute authorisation to transfer data pursuant to Article 69, paragraph 8, of the law of 6 January 1978 as amended.

Art. 6 – Personal data retention period

If the data controller considers that the personal data contained in a whistleblowing alert does not fall within the scope of the whistleblowing facility, it shall be destroyed or archived immediately.

If the whistleblowing alert does not lead to disciplinary action or legal proceedings, the personal data related to the alert shall be destroyed or archived by the organisation responsible for managing the alerts no later than two months after the verifications have been completed.

If disciplinary action or legal proceedings are taken against the person implicated or against a malicious whistleblower, the personal data contained in the whistleblowing alert shall be retained by the organisation responsible for the whistleblowing facility until the proceedings have ended.

Personal data that has been archived shall be retained in a separate restricted access information system, for a period not exceeding the duration of the legal or disciplinary proceedings.

Art. 7 – Security measures

The data controller shall take all precautionary measures to protect the security of the data, not only when it is received but also when it is transferred or stored.

More specifically, data may only be accessed via an individual user login and password, which are changed regularly, or by any other means of authentication. Access to data is recorded and the conformity of such access controlled.

The identity of the whistleblower and the persons implicated, as well as the information obtained by all recipients of the whistleblowing alert, shall be treated in the strictest confidence.

Art. 8 – Information to be provided to potential users of the whistleblowing facility

Clear and comprehensive information shall be provided to all potential users of the whistleblowing facility. Potential users include not only employees of the organisation, but also external and occasional workers.

In addition to the collective and individual information provided for in the French Labour Code and in accordance with Article 32 of the law of 6 January 1978 as amended, the information provided shall include the identity of the entity responsible for the whistleblowing facility, the objectives of the facility and the areas it covers, the fact that use of the facility is optional, that there shall be no negative consequences for non-use, that, where applicable, the personal data may be transferred to a country that is not a member of the European Union, and that the persons identified through the whistleblowing facility have a right to access, rectify and oppose the use of personal data about them.

The information shall also describe the steps of the whistleblowing facility, including how and to whom to send

a whistleblowing alert, in accordance with the provisions of Article 8 of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and economic modernisation.

It should be clearly indicated that abuse of the whistleblowing facility may lead to disciplinary action and legal proceedings, but, conversely, that if the facility is used in good faith, no penalties will be imposed on the whistleblower even if the facts subsequently prove to be incorrect or if no action is taken.

Art. 9 – Information to be provided to a person implicated in a whistleblowing alert

In accordance with Articles 6 and 32 of the law of 6 January 1978, a person implicated in a whistleblowing alert shall be notified by the person responsible for the whistleblowing facility as soon as the personal data is logged, electronically or otherwise, to enable that person to object to the processing of the personal data.

When protective measures are necessary, particularly to avoid the destruction of evidence related to a whistleblowing alert, the person implicated will only be notified once those measures have been taken.

This information shall be notified to the person implicated by any means that ensures due and proper delivery and such information shall specify the entity responsible for the whistleblowing facility, the allegations against the person implicated, the departments that have received the whistleblowing alert, if any, and the procedure for exercising the right to access and rectify the personal data received. The person implicated shall also be informed as required under Article 8 of this decision if this has not already been done.

Art. 10 – Compliance with the right to access and rectify personal data

In accordance with Articles 39 and 40 of the law of 6 January 1978 as amended, the person in charge of the whistleblowing facility shall ensure that anyone identified in a whistleblowing alert shall have the right to access their personal data and, if any of that information is incorrect, incomplete, unclear, or obsolete, ask for it to be rectified or deleted.

A person implicated in a whistleblowing alert may under no circumstances use this right of access to obtain information about the identity of the whistleblower from the data controller.

Art. 11 – Any whistleblowing facility providing for the processing of personal data that does not meet the provisions set out herein requires an application for authorisation from the Cnil in the form prescribed in Articles 25-I-3°, 25-I-4° and 30 of the law of 6 January 1978 as amended.

This deliberation amends deliberation No. 2005-305 of 8 December 2005 as last amended on 30 January 2014 and will be published in the "*Journal Officiel de la République Française*" (official gazette of the French Republic).

I. Falque-Pierrotin
The president

CODE OF ETHICS: THE KEY POINTS

In this Code of Ethics, Bouygues sets forth the core values it seeks to uphold, given its responsibilities to its customers, employees, shareholders, public- and private-sector partners and, in general, to civil society.

Bouygues expects all Group employees to comply with the following core values in the workplace:

1. **strict application of laws, regulations and internal standards,** in particular with regard to the protection of health, safety and the preservation of the environment;
2. **respect for employees,** in particular by complying with the Universal Declaration of Human Rights and the fundamental conventions of the International Labour Organisation (ILO);
3. **honesty, fairness and transparency** towards customers, shareholders and partners;
4. **accuracy and reliability** of internal control, accounts and financial information;
5. **compliance with the rules that ensure free competition, and rejection** of corruption in all its forms, in particular those prohibited by the OECD;
6. **loyalty to the company,** in particular by avoiding conflicts of interest, breaches of confidentiality and all prohibited stock market transactions involving listed Group securities;
7. **a team spirit** for intra-Group relations;
8. **protection of Group assets,** in particular by refraining from all personal possession or use;
9. **an ongoing concern to ensure quality and sustainable development;**
10. **political neutrality of the company,** the principle of prohibiting in particular all contributions to the financing of political activities.

BOUYGUES GROUP
32 avenue Hoche
F-75378 Paris cedex 08
Tel.: +33 (0)1 44 20 10 00
bouygues.com
Twitter: @GroupeBouygues

2006 • Updated: September 2017

The Bouygues group's Code of Ethics and Compliance Programmes (Competition, Anti-corruption, Financial Information and Securities Trading, Conflicts of Interest, and Embargoes and Export Restrictions) are available on the Group intranet (ByLink).

PEFC
10-31-3162

BOUYGUES