SPEAK UP POLICY

Approved

Version 11.0

ALL-POL-005

July 2025

INTERNAL

PREFACE

POLICY STATEMENT

Playtech is committed to conducting its business with honesty and integrity and to promoting a culture of openness, integrity and accountability.

An important aspect of this commitment to transparency is providing a way for staff and other members of Playtech to voice concerns about anything they find unsafe, unethical or unlawful. These mechanisms must be accessible, independent of line management, and must enable Personnel to voice concerns in a responsible, appropriate and effective manner without fear of criticism or retaliation.

This policy (the 'Speak Up Policy') is designed to support our values, our commitment to safeguard Personnel and to encourage Personnel to seek help and report any concerns they may have.

PURPOSE OF THIS POLICY

The purpose of this Policy is to:

- Encourage staff to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated, and that their confidentiality will be respected.
- Provide staff, business partners, contractors and suppliers with guidance as to how to raise those concerns.
- Reassure staff that they should be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistake
- Support other related policies including Playtech's Business Ethics Policy, Anti-Money Laundering and Counter-Terrorist Financing Policy, Anti-Facilitation of Tax Evasion Policy, Data Protection and Privacy Policy, Anti-Bribery and Corruption Policy, Wellbeing Policy and Human Rights Policy.

APPLICATION OF THIS POLICY

This Policy applies to the Playtech group of companies, which means Playtech Plc and its subsidiaries (collectively referred to as 'Playtech' in this Policy).

This Policy applies to all persons working for, or on behalf of, Playtech in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and where appropriate, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other persons associated with Playtech, wherever located. Collectively referred to as Personnel throughout this document.

This Policy does not form part of any employee's contract of employment and Playtech may amend it at any time.

OVERSIGHT AND MONITORING OF THIS POLICY

Playtech's Sustainability and Compliance Committee has overall responsibility for this Policy, and for reviewing the effectiveness of actions taken in response to concerns raised under this policy.

The Audit and Risk Committee will review this Policy regularly and at times when legislation or regulation changes that affects this Policy. The Regulatory Affairs and Compliance team ('Compliance') will report to the Audit and Risk Committee annually on the implementation of this Policy as well as the number and types of disclosures.

Playtech's Chief Compliance Officer has primary and day-to-day responsibility for implementing this Policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in supporting Personnel who wish to speak up.

Each entity within the Playtech group of companies (and its internal compliance function) is responsible for that entity's implementation of this Policy. Senior management, at all levels, are responsible for ensuring that those reporting to them are made aware of and understand this Policy.

Personnel are invited to comment on this Policy and suggest ways in which it may be improved. Comments, suggestions and queries should be addressed to Compliance.

Related Documents

Appendix A lists all documents which relate to or reference this Policy.

CONTENTS

1 SPEAKING UP

1.1 WHAT IS SPEAKING UP?

Speaking up, or whistleblowing, is raising genuine concerns about suspected unsafe, unethical or unlawful behavior at work. This may include (but is not limited to):

- Criminal activity;
- Failure to comply with any legal obligation or regulatory requirement;
- Danger to health, safety and/or employee safeguarding concerns under Playtech's Wellbeing Policy;
- Damage to the environment;
- Human rights and/or modern slavery breaches contrary to Playtech's Human Rights Policy;
- Bribery contrary to Playtech's Anti-Bribery and Corruption Policy;
- Facilitation of tax evasion contrary to Playtech's Anti-Facilitation of Tax Evasion Policy;
- Financial fraud or mismanagement;
- Negligence;
- Unethical behavior contrary to Playtech's Business Ethics Policy;
- Money laundering contrary to Playtech's Anti-Money Laundering and Counter-Terrorist Financing Policy;
- Conduct likely to damage Playtech's reputation;
- Unauthorised disclosure of confidential information or other data breaches contrary to Playtech's Data Protection and Privacy Policy;
- Bullying or sexual harassment; or
- The deliberate concealment of any of the above.

This is not an exhaustive list. If there is anything else that is causing Personnel concern, or that Playtech should be aware of, please do speak up.

However, this Speak Up Policy should not be used to:

- Question financial or business decisions taken by Playtech.
- Raise concerns relating to an employee's personal circumstances, such as the terms of their contract. In those cases, the employee should use the Grievance Procedure, which can be found in the employee handbook and/or by asking the People & Culture (P&C') Department for the procedure;
- Reopen matters that have already been addressed under Playtech's harassment, disciplinary or other procedures; or
- Make inaccurate, malicious or vexatious allegations. If an employee makes such complaints, and particularly if they persist with making them, disciplinary action may be taken against them.

If Personnel are uncertain whether something is within the scope of this Policy, they should seek advice from the Compliance group.

2 RASING A CONCERN

2.1 HOW TO RAISE A CONCERN

Playtech hopes that in many cases Personnel will be able to raise any concerns with their line manager, or local People & Culture or business unit representative. Personnel may raise a concern in person or put the matter in writing and should state that they are raising a concern under the Speak Up Policy. The line manager may be able to agree a way of resolving the concern quickly and effectively.

We would hope that you feel able to report internally to one of the contacts above within Playtech. However, if the nature of the matter is such that you cannot raise it with any of the contacts identified above or, if you have followed the internal channels listed above and you still have concerns, you can contact our confidential external 'Speak Up Line'. The Speak Up Line is an independent external hotline provided by Convercent for Playtech which allows Personnel across the Playtech group to raise concerns in their native language via telephone or via a secure web portal. From there, your report will be passed to Playtech and be dealt with in accordance with this Speak Up Policy.

2.2 WHAT HAPPENS WHEN A CONCERN IS RAISED

1. When an employee raises a concern (whether by contacting the Chief Compliance Officer, the General Counsel, the Global Director of People & Culture, or via the Speak Up Line), the details are channeled to the Chief Compliance Officer and General Counsel to investigate further.
2. Where appropriate, the Chief Compliance Officer and General Counsel may assign a team to conduct an investigation to gather and establish relevant facts relating to the matter. This may include the appointment of an independent, external legal advisor to support the review. Personnel may also be asked to provide further information, or answer questions about their concern, if required.
3. Personnel will receive an initial response to acknowledge receipt of their concern. From there, the Chief Compliance Officer, General Counsel or their appointed investigating lead will provide regular feedback and updates on the progress of the investigation into their concern until the matter has been resolved. If you contact the external Speak Up Line, you will receive a unique case number, which you can use to check the status of your concern and/or add additional information.
4. Playtech will use its best efforts to finalise the investigation process as soon as possible, but the duration of an investigation can vary depending on the complexity and severity of the concern raised. Playtech aims to resolve all matters, and to provide feedback to the employee, as soon as reasonably possible following the report.
5. Following the investigation, the investigating lead will produce a written report on the matter containing the findings of the investigation, the reasoning behind the decision and recommendations to address the issue. The report may be shared with the Chair of the Audit and Risk Committee of the Board and with the Chief Executive and Chairman, if appropriate.
6. Once the relevant members of senior management have been informed and consulted without compromising any confidentiality, the Chief Compliance Officer and General Counsel will implement the relevant actions required to resolve the matter, which could include disciplinary and/or other actions.
7. Where possible, the employee will be informed of the outcome of any investigations carried out and any actions taken, although confidentiality requirements may prevent this in some cases.
8. If there is evidence of criminal activity, the Chief Compliance Officer and General Counsel may consult external legal counsel and may report to the relevant law enforcement authorities. Playtech will ensure that any internal investigation does not hinder a formal police investigation.
9. Playtech will make every effort to address Personnel' concerns confidentially, fairly and professionally. If Personnel are not happy with the way in which a concern has been handled, they can contact any of the contacts listed in the section How to Raise a Concern.

10. If Playtech concludes that Personnel have made false allegations maliciously, Personnel may be subject to disciplinary action.

2.3 Confidentiality and Anonymity

Playtech will treat all concerns and disclosures made under this Policy in a confidential and sensitive manner and will treat any information with respect.

Personnel may choose to remain anonymous when raising a concern (subject to any local laws which prevent anonymous whistleblowing. If an employee wishes to remain anonymous when raising a concern (where permitted), they should make this clear upfront. Personnel may also contact Playtech's external Speak Up Line. The Speak Up Line will not attempt to trace their contact details and is legally forbidden from supplying an employee's details to Playtech without their explicit permission.

Playtech does not encourage Personnel to raise concerns anonymously. Proper investigation may be more difficult or impossible if we cannot obtain further information from the employee who raised the concern. It is also more difficult to establish whether the allegations are credible.

For those reasons, Playtech encourages Personnel to include their name in any disclosures. Playtech will only make the employee's name known to those people who need to know it in order to investigate the allegation or otherwise as required by law.

It is possible that the investigation process may reveal the source of the information. Alternatively, the employee making the disclosure may need to provide a statement as part of the evidence required. In the event such disclosure is necessary, this will be discussed with the employee beforehand, and the information will only be communicated with the investigating lead charged with looking into and resolving the concern.

2.4 Protection and Support For Speaking Up

It is understandable that Personnel who speak up may be concerned about possible repercussions and/or retaliation against them.

Playtech aims to encourage openness and will support staff who raise genuine concerns under this policy, even if the concerns are mistaken.

Playtech will do everything in its power to ensure that Personnel who speak up do not suffer any detrimental treatment as a result of raising a genuine concern. Detrimental treatment includes bullying, dismissal, disciplinary action, threats or other unfavorable treatment connected with raising a concern.

No employee should threaten or retaliate against those who speak up in any way. Anyone who is involved in such conduct may be subject to disciplinary action.

Retaliation can include the following types of actions: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; (l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; (m) early termination or cancellation of a contract for goods or services; (n) cancellation of a license or permit; (o) psychiatric or medical referrals.

Under the EU Whistleblowing Directive (Directive (EU) 2019/1937), UK Enterprise and Regulatory Reform Act 2013 and other relevant national regulatory frameworks in the different jurisdictions, greater protection for those who speak up has been introduced, including increased liability for instances where Personnel experience retaliation as a result of speaking up. Employers can now be held vicariously liable for the retaliatory actions of their Personnel, and those Personnel who make threats, victimise, or degrade whistleblowers (for example, through malicious allegations and other abuses of this Policy) can be held personally liable for their actions.

If Personnel believe that they have suffered detrimental treatment, they should inform the Chief Compliance Officer, General Counsel, Global Director of People and Culture or the Speak Up line immediately.

2.5 External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating, and remedying any wrongdoing in the workplace. The law recognises that in some circumstances it may be appropriate for Personnel to report concerns to an external body such as a regulator; however, Playtech strongly encourages Personnel to seek advice before reporting a concern to external organizations.

Concerns may relate to staff as well as the actions of a third party, such as a customer, supplier, or service provider. In some circumstances, the law will protect Personnel if raising a matter with the third party directly. However, Playtech encourages Personnel to report such concerns internally first. Personnel should contact their line manager, P&C, the Chief Compliance Officer and/or the General Counsel if they're unsure whether or not they wish to raise a concern under this policy or make an external disclosure.

2.6 Data Protection and Record Keeping

Playtech will keep all necessary records of concerns received and actions taken to investigate and remediate them. All records will be kept confidential and stored securely.

Any personal data received in connection with a speak up report will be handled in a manner that is compliant with Playtech's Data Protection and Privacy Policy.

2.7 Training and Awareness

Personnel will receive ongoing information about the mechanisms for speaking up, including the independent and confidential Speak Up line, and the protections provided to them under this Policy and through national laws and regulations. This information will be communicated via the new employee induction materials, company SharePoint, employee handbooks and compliance training modules.

Individuals responsible for supporting the Speak Up Policy, P&C focal points and relevant Legal and Compliance staff, will receive training about their obligations under this Policy and the underlying regulatory requirements.

The Compliance team is responsible for ensuring that relevant information about the Speak Up Policy and mechanisms is included in annual compliance training. The P&C function is responsible for ensuring that Personnel are provided with information about the Policy and speak up mechanisms.

APPENDIX A - RELATED DOCUMENTS

- Business Ethics Policy
- Anti-Bribery and Corruption Policy
- Anti-Facilitation of Tax Evasion Policy
- Data Protection and Privacy Policy
- Anti-Money Laundering and Counter-Terrorist Financing Policy
- Human Rights and Modern Slavery Statement
- Wellbeing Policy

ANNEX 1 - AUSTRALIA

1. INTRODUCTION

Playtech's Speak Up Policy (the **Policy**) reflects its global commitment to conducting business with honesty and integrity and to promoting a culture of openness, integrity and accountability.

The Policy applies within Australia in relation to Playtech's Australian subsidiaries and Personnel, but it is supplemented by this Annexure which is intended to ensure full compliance with specific Australian laws and requirements.

This Annexure explains when specific legal protections for whistleblowers will apply under the Corporations Act 2001 (Cth) (**Act**), what those protections are, and other relevant matters required by the Act.

The matters set out in this Annexure are not intended to detract from any rights or protections provided under the Policy or to limit the ways in which complaints can be made.

The definitions in the Policy apply to this Annexure.

2. APPLICATION OF POLICY

The Policy applies to an individual who is, or has been, any of the following in relation to Playtech's Australian subsidiaries (Eligible Whistleblowers):

- An officer or employee (e.g. current and former employees who are permanent, part-time, fixed-term or temporary, interns, secondees, managers, and directors);
- A supplier of services or goods to the entity (whether paid or unpaid), including their employees (e.g. current and former contractors, consultants, service providers and business partners);
- An associate of the relevant entity; and
- A relative, dependant or spouse of an individual referred to in the above paragraphs (e.g. relatives, dependants or spouses of current and former employees, contractors, consultants, service providers, suppliers and business partners).

3. WHEN IS 'SPEAKING UP' A DISCLOSURE TO WHICH THE ACT MAY APPLY?

Without limiting the meaning of speaking up in section 1.1 of the Policy, speaking up includes disclosing information where there are reasonable grounds to suspect that the information meets one or more of the following criteria (**Disclosable Matter**):

- It concerns misconduct (including fraud, negligence, default, breach of trust and breach of duty), or an improper state of affairs or circumstances, in relation to Playtech; or
- It indicates that Playtech, or an officer or employee of the Playtech, has engaged in conduct that:
  - constitutes an offence against, or a contravention of:
    - the Act;
    - the *Australian Securities and Investments Commission Act 2001* (Cth);
    - the *Banking Act 1959* (Cth), the *Financial Sector (Collection of Data) Act* 2001 (Cth), the *Insurance Act 1973* (Cth), the *Life Insurance Act 1995* (Cth), the *National Consumer Credit*

Protection Act 2009 (Cth), or the *Superannuation Industry (Supervision) Act 1993* (Cth), or instruments made under these laws; or

- constitutes an offence against any other federal law that is punishable by imprisonment for a period of 12 months or more; or
- represents a danger to the public or the financial system.

4. How to raise a concern so that protections may apply under the Act

Personnel may speak up in any way specified by the Policy, but this Annexure explains the circumstances in which making a disclosure will attract special additional protections under the Act.

Without limiting the persons to whom a disclosure may be made under the Policy, an Eligible Whistleblower may make a disclosure directly to an individual who is any of the following, in relation to any Australian Playtech subsidiary (**Eligible Recipients**):

- An officer or senior manager of the entity or a "related body corporate" within the meaning of the Act (**Related Body Corporate**);
- The internal or external auditor (including a member of an audit team conducting an audit) or actuary of the entity or a Related Body Corporate; and
- A person authorised by the entity to receive disclosures that may qualify for protection.

5. Disclosures that attract protection under the Act

When does speaking up qualify for specific protection under the Act?

Without limiting the rights of any Personnel under the Policy to speak up in accordance with the Policy, speaking up will only attract the specific whistleblower protections under the Act where a disclosure is made by an Eligible Whistleblower in one of the following circumstances:

Disclosure to Eligible Recipient or government authority

The disclosure is made in relation to a Disclosable Matter and directly to:

- An Eligible Recipient; or
- The Australian Securities and Investments Commission (ASIC), the Australian Prudential Regulation Authority (APRA) or another Commonwealth body prescribed by the relevant regulations; or

Disclosure to legal practitioner seeking advice

The disclosure is made to a legal practitioner for the purposes of obtaining legal advice or representation in relation to the operation of the whistleblower provisions in the Act (this protection applies even if the legal practitioner concludes that a disclosure does not relate to a Disclosable Matter); or

Public interest or emergency disclosure

The disclosure is made in accordance with the requirements for a 'public interest disclosure' or 'emergency disclosure', as explained below.

What is a public interest disclosure?

A 'public interest disclosure' is the disclosure of information to a journalist or a parliamentarian, where:

- At least 90 days have passed since the discloser made the disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation; and

- The discloser does not have reasonable grounds to believe that action is being, or has been taken, in relation to their disclosure; and
- The discloser has reasonable grounds to believe that making a further disclosure of the information is in the public interest; and
- Before making the public interest disclosure, the discloser has given written notice to the body to which the previous disclosure was made that:
    - Includes sufficient information to identify the previous disclosure; and
    - States that the discloser intends to make a public interest disclosure.

What is an emergency disclosure?

An 'emergency disclosure' is the disclosure of information to a journalist or parliamentarian, where:

- The discloser has previously made a disclosure of the information to ASIC, APRA or another Commonwealth body prescribed by regulation; and
- The discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment; and
- Before making the emergency disclosure, the discloser has given written notice to the body to which the previous disclosure was made that: and
    - Includes sufficient information to identify the previous disclosure; and
    - States that the discloser intends to make an emergency disclosure; and
- The extent of the information disclosed in the emergency disclosure is no greater than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

Disclosure that turns out to be incorrect

An Eligible Whistleblower who makes a disclosure that turns out to be incorrect can still qualify for protection under the Act if they had reasonable grounds to suspect that their disclosure was true and met the definition of a Disclosable Matter in section 3.1 of this Annexure.

Personal work-related grievances generally don't qualify for protection under the Act

Without limiting any rights to speak up under the Policy, disclosures relating to personal work-related grievances generally do not qualify for any special protection under the Act.

Examples of personal work-related grievances include:

- An interpersonal conflict between the discloser and another employee;
- A decision that does not involve a breach of workplace laws;
- A decision about the engagement, transfer or promotion of the discloser;
- A decision about the terms and conditions of engagement of the discloser; or
- A decision to suspend or terminate the engagement of the discloser, or to otherwise discipline the discloser.

Circumstances where disclosure of personal work-related grievance may be protected

In limited circumstances, a personal work-related grievance may still qualify for protection under the Act, including if:

- It includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report);

- A Playtech entity has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct (within the meaning of the Act – see section 3.1(a) of this Annexure) beyond the discloser's personal circumstances; or
- The discloser suffers from or is threatened with detriment in a manner prohibited by the Act in relation to an actual, suspected or proposed disclosure (see sections 6.6 and 6.7 of this Annexure), and their grievance relates to such a detriment or threat.

6. WHAT ARE THE SPECIFIC WHISTLEBLOWER PROTECTIONS UNDER THE ACT?

Without limiting the protections contained in the Policy, the following protections are specified under the Act for disclosures that meet the requirements specified by the Act and explained in section 5 of this Annexure.

Identity protection (confidentiality)

Except in the circumstances specified in section 6.3 of this Annexure, a person cannot disclose the identity of a discloser, or information that is likely to lead to the identification of the discloser, which they have obtained directly or indirectly because the discloser made a disclosure that qualifies for protection.

A person may disclose the identity of a discloser:

- To ASIC, APRA, or a member of the Australian Federal Police within the meaning of the *Australian Federal Police Act 1979* (Cth);
- To a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Act;
- To a person or body prescribed by the relevant regulations; or
- With the consent of the discloser.

Under the Act, a person is permitted to disclose the information contained in a disclosure with or without the discloser's consent if:

- The information does not include the discloser's identity;
- The entity has taken all reasonable steps to reduce the risk that the discloser will be identified from the information; and
- It is reasonably necessary for investigating the issues raised in the disclosure.

Under the Act, it is unlawful for a person to identify a discloser, or disclose information that is likely to lead to the identification of the discloser, outside the exceptions specified in this Annexure.

Protection from detrimental acts or omissions

Under the Act, a person cannot engage in conduct that causes detriment to a discloser (or another person), in relation to a disclosure, if:

- The person believes or suspects that the discloser (or another person) made, may have made, proposes to make or could make a disclosure that qualifies for protection under the Act; and
- The belief or suspicion is the reason, or part of the reason, for the conduct.

In addition, a person cannot make a threat to cause detriment to a discloser (or another person) in relation to a disclosure. A threat may be express or implied, or conditional or unconditional. A discloser (or another person) who has been threatened in relation to a disclosure does not have to actually fear that the threat will be carried out.

Section 2.4 of the Policy provides examples of detriment (described as “retaliation”) that would be unlawful under the Act.

Compensation and other remedies

A discloser (or any other employee or person) can seek compensation and other remedies through the courts if:

- They suffer loss, damage or injury because of a disclosure that meets the requirements for protection under the Act, as explained in this Annexure; and
- Playtech failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

Civil, criminal and administrative liability protection

A discloser is protected from any of the following in relation to a disclosure that meets the requirements for protection under the Act, as explained in this Annexure:

- Civil liability (e.g. any legal action against the discloser for breach of an employment contract, duty of confidentiality or another contractual obligation);
- Criminal liability (e.g. attempted prosecution of the discloser for unlawfully releasing information, or other use of the disclosure against the discloser in a prosecution, other than for making a false disclosure); and
- Administrative liability (e.g. disciplinary action for making the disclosure).

The protections under the Act do not grant immunity for any misconduct a discloser has engaged in that is revealed in their disclosure.

7. Support and Practical Protection For Disclosers

The Policy includes information about other measures available to support disclosers, including by protecting their identity, ensuring confidentiality and protecting disclosers from detriment (described as “retaliation” in the Policy).

8. Anonymity

For the avoidance of doubt, a person who speaks up anonymously in accordance with the Policy will still be entitled to protection if their disclosure meets the requirements for protection under the Act, which are explained in this Annexure.

A discloser may choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalised. The Policy provides further details on anonymous disclosures, including details regarding Playtech’s confidential, external “Speak Up Line”.

9. Ensuring the Policy and Annexure are easily accessible

The training and awareness measures specified in section 2.7 of the Policy will also apply to this Annexure in relation to Playtech’s Australian subsidiaries and Personnel.

ANNEX 2 - AUSTRIA

The Speak Up Policy is amended for persons within the scope of application of this policy working in and protected by the laws of the Republic of Austria, in order to comply with the Austrian Act on the Protection of Whistleblowers (Federal Gazette I Nr. 6/2023, HinweisgeberInnenschutzgesetz – HSchG).

Such clauses are replaced as follows (amended wording marked up in **bold**):

Clause	Replacing Text (Amendments Underlined)
Application of this Policy	This Policy applies to the Playtech group of companies, which means Playtech Plc and its subsidiaries (collectively referred to as 'Playtech' in this Policy). This Policy applies to applicants, all persons working for, or on behalf of, Playtech in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, trainees, and where appropriate, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other persons associated with Playtech, including shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, wherever located. Collectively referred to as Personnel throughout this document. This Policy does not form part of any employee's contract of employment and Playtech may amend it at any time.
1.1	Speaking up, or whistleblowing, is raising genuine concerns about suspected unsafe, unethical or unlawful behaviour at work. This may include (but is not limited to): ▪ Criminal activity; ▪ Failure to comply with any legal obligation or regulatory requirement, **including product safety and conformity, transport safety, food and feed safety, animal health, animal welfare, public health, harm to the financial interests of the EU and the violation of EU single market rules**; ▪ Danger to health, safety and/or employee safeguarding concerns under Playtech's Wellbeing Policy; ▪ Damage to the environment; ▪ Human rights and/or modern slavery breaches contrary to Playtech's Human Rights Policy; ▪ Bribery contrary to Playtech's Anti-Bribery and Corruption Policy; ▪ Facilitation of tax evasion contrary to Playtech's Anti-Facilitation of Tax Evasion Policy; ▪ Financial fraud or mismanagement; ▪ Negligence; ▪ Unethical behavior contrary to Playtech's Business Ethics Policy; ▪ Money laundering contrary to Playtech's Anti-Money Laundering and Counter-Terrorist Financing Policy; ▪ Conduct likely to damage Playtech's reputation; ▪ Unauthorised disclosure of confidential information or other data breaches contrary to Playtech's Data Protection and Privacy Policy, **including the security of network and information security systems**; ▪ **Infringements of fair competition, public procurement and state aid rules**; ▪ Bullying or sexual harassment; or ▪ The deliberate concealment of any of the above.

Clause	Replacing Text (Amendments Underlined)
	This is not an exhaustive list. If there is anything else that is causing Personnel concern, or that Playtech should be aware of, please do speak up. However, this Speak Up Policy should not be used to: ▪ Question financial or business decisions taken by Playtech; ▪ Raise concerns relating to an employee's personal circumstances, such as the terms of their contract. In those cases, the employee should use the Grievance Procedure, which can be found in the employee handbook and/or by asking the People & Culture ('P&C') Department for the procedure; ▪ Reopen matters that have already been addressed under Playtech's harassment, disciplinary or other procedures; or ▪ Make inaccurate, malicious or vexatious allegations. If an employee makes such complaints, and particularly if they persist with making them, disciplinary action may be taken against them. If Personnel are uncertain whether something is within the scope of this Policy, they should seek advice from the Compliance group.
2.2	1. When an employee raises a concern (whether by contacting the Chief Compliance Officer, the General Counsel, the Global Director of P&C, or via the Speak Up Line), the details are channeled to the Chief Compliance Officer and General Counsel to investigate further. Where appropriate, the Chief Compliance Officer and General Counsel may assign a team to conduct an investigation to gather and establish relevant facts relating to the matter. This may include the appointment of an independent, external legal advisor to support the review. Personnel may also be asked to provide further information, or answer questions about their concern, if required. **Personnel may also request a meeting in person (or e-meeting), which will be complied with within 14 calendar days**. Personnel will receive an initial response to acknowledge receipt of their concern, **unless Personnel has expressly objected or there are reasons to assume that response would compromise the confidentiality of the identity**. From there, the Chief Compliance Officer, General Counsel or their appointed investigating lead will provide regular feedback and updates on the progress of the investigation into their concern until the matter has been resolved. If you contact the external Speak Up Line, you will receive a unique case number, which you can use to check the status of your concern and/or add additional information. Playtech will use its best efforts to finalise the investigation process as soon as possible, but the duration of an investigation can vary depending on the complexity and severity of the concern raised. Playtech aims to resolve all matters, and to provide feedback to the employee, as soon as reasonably possible following the report. Following the investigation, the investigating lead will produce a written report on the matter containing the findings of the investigation, the reasoning behind the decision and recommendations to address the issue. The report may be shared with the Chair of the Audit and Risk Committee of the Board and with the Chief Executive and Chairman, if appropriate. Once the relevant members of senior management have been informed and consulted without compromising any confidentiality, the Chief Compliance Officer and General Counsel will implement the relevant actions required to resolve the matter, which could include disciplinary and/or other actions.

Clause	Replacing Text (Amendments Underlined)
	Where possible, the employee will be informed of the outcome of any investigations carried out and any actions taken, although confidentiality requirements may prevent this in some cases. **In any case, Personnel will be informed no later than three months after receipt of the concern as to what follow-up measures have been or will be taken or for what reasons the concern will not be investigated further**. If there is evidence of criminal activity, the Chief Compliance Officer and General Counsel may consult external legal counsel and may report to the relevant law enforcement authorities. Playtech will ensure that any internal investigation does not hinder a formal police investigation. Playtech will make every effort to address Personnel' concerns confidentially, fairly and professionally. If Personnel are not happy with the way in which a concern has been handled, they can contact any of the contacts listed in the section How to Riase a Concern . If Playtech concludes that Personnel have made false allegations maliciously, Personnel may be subject to disciplinary action.
2.3	Playtech will treat all concerns and disclosures made under this Policy in a confidential and sensitive manner and will treat any information with respect. If a concern is raised with a line manager, or local P&C or business unit representative or any other person or entity not the Chief Compliance Officer, General Council or the Speak Up Line, they are prohibited from disclosing the content of the concern or identity of the concern raising Personnel to third parties and obliged to forward the concern to the Chief Compliance Officer. Personnel may choose to remain anonymous when raising a concern (subject to any local laws which prevent anonymous whistleblowing. If an employee wishes to remain anonymous when raising a concern (where permitted), they should make this clear upfront. Personnel may also contact Playtech's external Speak Up Line. The Speak Up Line will not attempt to trace their contact details and is legally forbidden from supplying an employee's details to Playtech without their explicit permission. Playtech does not encourage Personnel to raise concerns anonymously. Proper investigation may be more difficult or impossible if we cannot obtain further information from the employee who raised the concern. It is also more difficult to establish whether the allegations are credible. For those reasons, Playtech encourages Personnel to include their name in any disclosures. Playtech will only make the employee's name known to those people who need to know it in order to investigate the allegation or otherwise as required by law. It is possible that the investigation process may reveal the source of the information **if an administrative authority, a court or the public prosecutor's office considers this to be essential in the context of investigations or proceedings and proportionate in view of the risk to the reporting Personnel, the validity and seriousness of the allegations made**. Alternatively, the **Personnel** making the disclosure may need to provide a statement as part of the evidence required. In the event such disclosure is necessary, this will be discussed with the **Personnel** beforehand, and the information will only be communicated with the investigating lead charged with looking into and resolving the concern.

ANNEX 3 - BULGARIA

The aim of this ANNEX is to adapt this part of the Policy which does not reflect specific legal requirements in Bulgaria and to supplement its provisions, where applicable. This ensures that the whistleblowing process in Playtech Bulgaria aligns with local legal requirements and provides clear guidance for employees operating within this jurisdiction.

The following sections outline the specific adaptations and provisions applicable under Bulgarian law, including the mechanisms for reporting concerns, protections available to whistleblowers, and any procedural differences from the global Speak Up Policy. This information is intended to help employees understand their rights and the processes in place to support and protect them when reporting misconduct.

Application of this Annex

This ANNEX applies to the Personnel of Playtech Bulgaria Ltd., registered under company number 175110853, having its management address in Sofia 1784, 115l Tsarigradsko shose Blvd., European Trade Center, building C, floor 6-7.

For the avoidance of doubt and for the purposes of this ANNEX, the Personnel referenced in the Speak Up Policy shall include persons working for, or on behalf of, Playtech Bulgaria in any capacity. In addition to the capacities listed in the Speak Up Policy, Personnel shall also include any person engaged by Playtech Bulgaria, having the status of a self-employed person, including a person working without an employment relationship and/or exercising a freelance profession and/or performing activity in the field of crafts/artisanry; a representative of the sole owner of Playtech Bulgaria's capital/Playtech Bulgaria's shareholder and/or a manager of Playtech Bulgaria; a person who works for Playtech Bulgaria's contractors or for the contractor's subcontractors or suppliers; job applicants in cases where information regarding breaches was obtained during the recruitment process or other pre-contractual relationship with Playtech Bulgaria; and former employees, where the information was obtained in the context of an employment relationship with Playtech Bulgaria that had been terminated at the time of the report or public disclosure. Each of the individuals noted in this paragraph can have the role of a **Reporting Person** within the meaning of this ANNEX.

1. SPEAKING UP

To ensure compliance with Bulgarian law, adjustments have been made to the scope of the Speak Up Policy. Any reported concerns which are out of scope of the Bulgarian whistleblowing regulations and the process set up under this ANNEX, may be reviewed by Playtech under the general terms of the global Speak Up Policy or any specific local legislation as the case may be, and the adaptations under this ANNEX shall not apply.

The clauses of **paragraph 1** have been replaced as follows:

1.1 WHAT IS SPEAKING UP IN BULGARIA?

Speaking up, or whistleblowing, is raising genuine concerns about the following infringements ("**Breaches**"):

- Infringements of Bulgarian legislation or of European Union acts in the field of:
  - Public procurement;
  - Financial services, products and markets and the prevention of money laundering and terrorist financing;
  - Product safety and compliance;
  - Transport safety;

- Environmental protection;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and animal welfare;
- Public health;
- Consumer protection;
- The protection of privacy and personal data;
- Security of networks and information systems;

- Infringements affecting the financial interests of the European Union;
- Infringements of European Union internal market rules, including European Union's and Bulgaria's rules regarding competition and state aid;
- Breaches relating to cross-border tax schemes designed to obtain a tax advantage contrary to the object or purpose of the applicable corporate tax law;
- A criminal act of a general nature that has been committed of which Personnel has become aware in connection with the performance of his/her work.
- Violations of Bulgarian legislation regulating:
  - The rules for payment of due public state and municipal debts (e.g. taxes, social security contributions, local taxes);
  - Labour legislation;
  - Legislation relating to the performance of public service.

However, without prejudice to the items listed in Paragraph 1.1. of the Speak Up Policy, the following reports shall be excluded from the application of this ANNEX:

- Anonymous reports (with some exceptions) – please refer to section 2.3.3. for more details on anonymous reports;
- Reports that concern a complaint or claim from customers/users in relation to services provided by Playtech Bulgaria - may be accepted, but not registered and handled under this ANNEX;
- Reports relating to Breaches committed more than two years ago, provided that such limitation continues to exist under the *Bulgarian Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches* ("the Bulgarian Whistleblowing Act ") and that the proper actions were taken to review the report and establish the time of the commission of the Breach;
- Reports which concern only interpersonal relations, regardless of the presence or absence of a work context;
- Other reports excluded by the relevant legislation such as Art. 4 of the Bulgarian Whistleblowing Act.

2. RAISING A CONCERN

To ensure compliance with Bulgarian law, adjustments have been made to the process of raising a concern under the Speak Up Policy for this jurisdiction and in relation to Playtech Bulgaria's activities.

The clauses of **paragraph 2.1** have been replaced as follows:

2.1 How to Raise a Concern (report)

In Bulgaria, Playtech Bulgaria has established a specific channel ("**Internal Reporting Channel**") to receive written and verbal reports of breaches as required by the Bulgarian Whistleblowing Act. Raising a concern (report) on a Breach should be submitted in writing via email to the following email address: SpeakUp.Bulgaria@playtech.com. Raising a concern may also be made verbally by meeting with a in person at Playtech Bulgaria's office at 1784 Sofia, 115L Tsarigradsko Shosse Blvd., European Trade Center, Entrance C, floor 6-7 at a pre-arranged time for a meeting with the specific person who is responsible for receiving, registering and handling of concerns received under the Bulgarian Whistleblowing Act and the Speak Up Policy in Bulgaria ("**Responsible Person**"). The Responsible Persons for Bulgaria are:

- Martina Dixey, Senior Compliance Manager
- Nayda Teneva, Sanctions Manager
- Daria Topalova, Senior People & Culture Director

The raised concern (report) must contain the following details, preferably filled in by the Reporting Person in a form for registering a report (the "Form" (see template at https://cpdp.bg/en/form-for-registering-a-report-under-whistleblowers-protection-act/.):

- Details of the Reporting Person – full name and contact details;
- Details of the natural or legal person against whom the report is made ("Person Concerned") and his/her place of work;
- An electronic or handwritten signature of the Reporting Person, unless the report is made verbally;
- Date or period of the Breach;
- Sufficient and convincing evidence which leads to the conclusion that it is likely that the alleged Breach has occurred and it is covered by the conditions in Paragraph 1.1. above;
- Specific details of the Breach or of a real risk of a Breach being committed, the place and period of the Breach, if any;
- A description of the act or the setting and such other circumstances as are known to the Reporting person.

The absence of the above conditions results in an irregular report and the Responsible Person will inform the Reporting Person of the irregularities found and will give him/her a 7-day period to remedy them. Depending on the nature of the irregularity, the Responsible Person may also request clarification in communications with the Reporting Person of the details and circumstances of the report.

The raised concern (report) must not contain demonstrably false or misleading statements of fact. In such a case, instructions are returned to the Reporting Person to clarify the allegations, informing them of their liability for incrimination.

The clauses of paragraph 2.2 have been replaced as follows:

2.2 What happens When a Concern is Raised

2.2.1 Registering the concern (report)

Receipt of a report through Playtech Bulgaria's established Internal Reporting Channel is done by placing a serial registration number and date according to the incoming correspondence and a reports log is kept by the Responsible Persons.

Playtech Bulgaria has established and maintains a register of the reports of Breaches ("**Register of Reports**"), accessible only by the Responsible Persons and the relevant regulatory authorities in accordance with the Bulgarian Whistleblowing Act.

Received reports, insofar as they are subject to further processing under the Bulgarian Whistleblowing Act and this ANNEX, are registered by a Responsible Person through:

filling in a Form, if the Reporting Person has not already done so for the purposes of submitting the report;

- Entry in the Register of Reports with a serial number and date of submission;
- Generating a Unique Identification Number ("**UIN**") using the UIN generation functionality provided on the website of the Commission for Personal Data Protection ("**CPDP**");
- Sending an acknowledgement of receipt of the report to the Reporting Person, and (if applicable) instructions to rectify any irregularities in the report, within 7 days of receipt.

Immediately following the registration of the report in the Register of Reports, the Responsible Person verifies whether the report was submitted by a member of Personnel and whether it relates to Breaches covered by the Bulgarian Whistleblowing Act as described in Paragraph 1.1. of this ANNEX. If the report falls within the scope of the Bulgarian Whistleblowing Act, the Responsible Person immediately (within Playtech Bulgaria's business hours) takes action to generate a UIN using the UIN generation functionality provided on the CPDP website. For reports received after Playtech Bulgaria's business hours, the request for a UIN is made on the first business day following the receipt of the report.

2.2.2 Examination of The report

Prior to commencing work, the relevant Responsible Person ensures that s/he is not in a position of conflict of interest regarding the content of the report, the Reporting Person and/or any person associated with the report. If there is the slightest suspicion of a conflict of interest or a risk of a conflict of interest, the respective Responsible Person is not taking any further action on the report and passes the report file to other Responsible Persons.

After commencing work, the Responsible Person checks the existence of the conditions and requisites required or requests a remedy, if necessary, as provided under Paragraph 2.1. above. When this is completed, the Responsible Person initiates the handling of the report.

The handling of each report by the Responsible Person is concluded with the preparation of an individual written report on the raised concern, containing a brief description of the information, the actions taken and the final results of the verification of the report.

2.2.3 Actions Taken by Playtech

Playtech Bulgaria aims to resolve all matters and to provide feedback to the Reporting Person, as soon as reasonably possible following the report and no more than 3 months after the acknowledgement of receipt of the report.

- In the event that the facts presented in the report are confirmed, the Responsible Person:
- Arranges for follow-up action to be taken in relation to the report, and for this purpose may require the assistance of other persons within Playtech;
- Proposes to Playtech Bulgaria to take specific measures to stop or prevent the Breach in cases where such Breach has been detected or there is a real danger of its imminent commission;
- Refers the Reporting Person to the competent authorities where his or her rights are concerned;
- Forwards the report to the CPDP, if action is required on its part, and the Reporting Person is informed in advance of the forwarding.

Playtech Bulgaria takes the following subsequent actions:

- Action within its competence to stop the Breach or to prevent it, if it has not started;
- Prioritizes, according to criteria and rules established in advance by Playtech Bulgaria‘s management, the handling of multiple reports of more serious Breaches;
- Terminates the check:
  - When the Breach reported is a minor case and does not require further follow-up action;
  - On a repeat report that does not contain new information material to a Breach with respect to which an investigation has already been completed, unless new legal or factual circumstances warrant further action;
  - When evidence of a criminal offence has been established, in which case the report and the accompanying materials shall be sent immediately to law enforcement;
- Prepares an individual report, which describes the information from the report, the actions taken, the final results, which are communicated to the Reporting Person and to the Person Concerned by observing the confidentiality obligations under local law.

The clauses of **paragraph 2.3** have been replaced as follows:

2.3 CONFIDENTIALITY AND ANONYMITY

2.3.1 INTERNAL REPORTING CHANNEL

Playtech Bulgaria is managing the Internal Reporting Channel in a secure manner that ensures the completeness, integrity and confidentiality of the information. Playtech Bulgaria protects the identity of the Reporting Person and any third party named in the report and prevents unauthorised persons and staff members from accessing the report. To this end, Playtech Bulgaria implements technical and organisational measures, including as follows:

- The Internal Reporting Channel provides a direct link to the Responsible person. Playtech Bulgaria ensures that no other members of Playtech Bulgaria's staff (including the Legal Representative) have access to the report submitted, other than the Responsible Person;
- In the case of an in-person meeting with the Reporting Person, the meeting is held in a suitable location in Playtech Bulgaria's office that provides a sufficient degree of confidentiality, is separate from the other work areas where other employees work and is out of reach of CCTV systems in the office. At the discretion of the Responsible person, the in-person meeting may also be held outside of Playtech Bulgaria’s premises to ensure confidentiality;
- Playtech Bulgaria ensures that access to the submitted written reports, the attachments and materials provided with the reports, as well as any information collected in the course of the process of handling the reports is carried out strictly on a need-to-know basis and by closely observing the obligation of confidentiality, whereas full access to the identity of the Reporting Person and any other natural person specified in the report and in the completed Form for registration of the report are limited to the Responsible Person and the employees who need such data for the performance of their duties.
- The transmission of data and reference to circumstances relating to a Reporting Person by a Responsible Person shall not directly or indirectly reveal the identity of the Reporting Person or create an assumption as to the identity of the Reporting Person. Accordingly, the Responsible Person makes the necessary revisions to any material it provides to any third party to ensure that the identity of the Reporting Person and other persons involved in the report is protected;

Subject to the Bulgarian Whistleblowing Act, the identity of the Reporting person and any other information from which his/her identity may be directly or indirectly known may be disclosed only where this is a necessary and proportionate obligation imposed by Bulgarian or European Union law in the

context of investigations by national authorities or legal proceedings, including with regard to ensuring Playtech Bulgaria's rights of defense.

Exceptionally, limited information about the content of the report may be accessed by other employees and/or external consultants (e.g. lawyers, accountants) who need the data to perform their official and/or professional duties. In such cases, prior to disclosing the identity, Playtech Bulgaria notifies the Reporting Person or the Person Concerned, as the case may be, of the need to disclose the information relating to him in writing and in a reasoned manner. The Reporting Person/Person Concerned is not notified where doing so would jeopardise the investigation or legal proceedings.

2.3.2 Register of Reports

The information recorded in the Register of Reports is stored in a manner that ensures its confidentiality and security, subject to the appropriate application of the measures referred to in Paragraph 2.3.1. above. Only the Responsible Persons, the CPDP and other competent authorities under the law shall have access to the complete information stored in the Register of Reports.

A Responsible Person may provide Playtech Bulgaria with information from the Register of Reports only on condition that this does not lead to the disclosure of the identity of the Reporting Person and/or the Person Concerned, e.g. by submitting edited extracts from the Register of Reports, pseudonymisation, etc.

2.3.3 Anonymous Reports

Anonymous reports received by Playtech Bulgaria are generally not registered and handled under this ANNEX. Such reports are received by the Responsible Persons and may be reviewed and handled in accordance with the global process set up as per the global Speak Up Policy of Playtech.

By exception, an anonymous report may be registered and handled under this ANNEX if the Reporting Person has made an anonymous report or has publicly, but anonymously, disclosed information about Breaches but has subsequently been identified. In such cases, the Responsible Person verifies whether the anonymous report or the information made public meets the requirements of the Bulgarian Whistleblowing Act, namely:

- The Reporting Person had reasonable ground to believe that the information submitted about the Breach in the report was correct at the time it was submitted and that such information is covered by the Bulgarian Whistleblowing Act as described in Paragraph 1.1. of this ANNEX; and
- The Reporting Person has made a report under the terms and conditions of the Bulgarian Whistleblowing Act, but the report has not been acted upon within the statutory time limits; or
- The Reporting Person has reason to believe that:
  - The violation may constitute an imminent or obvious danger to the public interest or there is an emergency or risk of irreversible harm;
  - There is a risk of retaliation or the likelihood that the Breach will not be dealt with effectively because of the risk of concealment or destruction of evidence, suspicion of collusion between the competent authority and the perpetrator of the Breach, or complicity by the authority in the Breach, or other specific circumstances of the case.

The last paragraph of **paragraph 2.4** is amended as follows:

2.4 Protection and Support For Speaking Up

If Personnel of Playtech Bulgaria believe that they have suffered detrimental treatment, they should inform the Responsible Person appointed at Playtech Bulgaria or submit a report through the Internal Reporting Channel or the External Reporting Channel immediately.

The second paragraph of **paragraph 2.5** has been amended and a third paragraph is supplemented in **paragraph 2.5** as follows:

2.5 External Disclosures

Concerns may relate to staff as well as the actions of a third party, such as a customer, supplier, or service provider. The law will protect Personnel if raising a matter with the third party directly. However, Playtech Bulgaria encourages Personnel to report such concerns internally first. Personnel should contact the Responsible Persons appointed in Playtech Bulgaria if they're unsure whether or not they wish to raise a concern under this ANNEX or make an external disclosure.

The external reporting channel in Bulgaria is maintained by the Commission for Personal Data Protection (CPDP). The contact details for using the external reporting channel are as follows:

- In writing by email to: whistleblowing@cpdp.bg or by mail to: 1592, Sofia, 2 "Prof. Tsvetan Lazarov" Blvd.
- Orally on site at the CPDP at 1592, Sofia, 2 "Prof. Tsvetan Lazarov" Blvd.

For more information Personnel may refer to CPDP's webpage.

The clauses of **paragraph 2.6** have been amended as follows:

2.6 Data protection and Record Keeping

Playtech Bulgaria will keep all necessary information about the report and actions taken to investigate and remediate them. All records will be kept confidential and stored securely on a durable medium pursuant to the Bulgarian Whistleblowing Act.

Any personal data received in connection with a speak up report will be handled in a manner that is compliant with Playtech Bulgaria's Data Protection and Privacy Policy and Regulation (EU) 2016/679 (General Data Protection Regulation), as well as the Bulgarian Personal Data Protection Act.

The Register of Reports, the reports themselves and the materials attached to them, including subsequent documentation related to their handling, will be kept by Playtech Bulgaria for a period of 5 years after the completion of the examination of the report, except in the case of criminal, civil, labour and/or administrative proceedings initiated in connection with the submitted report. After the expiry of the retention period, the material will be destroyed as per Playtech Bulgaria's applicable policies.

The clauses of paragraph 2.7 have been amended as follows:

2.7 Training and Awareness

The clauses of **paragraph 2.7** remains unchanged under the Global Speak up policy.

ANNEX 4 - REPUBLIC OF CYPRUS

The Speak Up Policy is amended for those working in and protected by the law of Cyprus as the paragraphs set out below are not compliant with such legislation. The applicable law is the Law on the Protection of Persons Reporting Violations of Union and National Law 6(I)/2022 as amended or replaced from time to time, including secondary legislation (**Law**).

Such clauses are amended as follows:

- Subparagraph 2.2.3. will be amended to include the phrase '**within seven (7) days from the day of receipt of their concerns**' at the end of the first sentence. The sentence will therefore read as follows:

  'Personnel will receive an initial response to acknowledge receipt of their concern within seven (7) days from the day of receipt of their concerns. '

- Subparagraph 2.2.7. will be replaced as follows:
- *'Irrespective of the outcome of the investigation the Personnel will be notified about it within a reasonable time not exceeding three (3) months from the date of sending the acknowledgment of receipt. However, the need for confidentiality may prevent the Company from giving specific details of the investigation or any disciplinary action taken as a result.'*
- Clause 2.5. is amended to include the following paragraph at the end of clause 2.5 and add clause 2.5.1.:

  '*If the Personnel has filed an internal report in relation to a concern and whilst pending the Personnel decide to make an external report for the same concern, the Personnel is obliged to inform the internal proceeding channels of this report. In such event, the internal disclosure process will be interrupted.*'

- **2.5.1 Public Disclosure**

  Personnel is also entitled to make a public disclosure in relation to their concerns in accordance with the provisions of the Law.

ANNEX 5 - GERMANY

The Speak Up Policy is amended for those working in and protected by the laws of Germany with the following wording added to clause 2.4:

'Within the material scope of the application of the HinSchG, the protection of employees speaking up includes:

- The employee speaking up cannot be held liable for obtaining or accessing
- information that he/she has reported/disclosed unless procurement/access as such constitutes an independent criminal offence.
- The Employee speaking up does not violate any disclosure restrictions,
- provided they had reasonable grounds to believe that the disclosure of the information was necessary to uncover an offence.
- The prohibition of retaliation applies (see below). This also applies to the threat and
- attempt to take retaliation.
- In the event of disadvantage to the employee speaking up, it is assumed that the disadvantage is a retaliation if the employee speaking up invokes it. The person causing the disadvantage must prove that there are sufficiently justified reasons or that it was not based on the report or disclosure.
    - If the employee speaking up has suffered damage as a result of the retaliation, there is a claim for damages.'

EXCERPT FROM WHISTLEBLOWER PROTECTION ACT (HINSCHG)

§ 2 Sachlicher Anwendungsbereich

(1) Dieses Gesetz gilt für die Meldung (§ 3 Absatz 4) und die Offenlegung (§ 3 Absatz 5) von Informationen über

1. VerstöBe, die strafbewehrt sind,
2. VerstöBe, die buBgeldbewehrt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient,
3. sonstige VerstöBe gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union und der Europäischen Atomgemeinschaft
    a) zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, unter Einschluss insbesondere des Geldwäschegesetzes und der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006 (ABl. L 141 vom 5.6.2015, S. 1), die durch die Verordnung (EU) 2019/2175 (ABl. L 334 vom 27.12.2019, S. 1) geändert worden ist, in der jeweils geltenden Fassung,
    b) mit Vorgaben zur Produktsicherheit und -konformität,
    c) mit Vorgaben zur Sicherheit im StraBenverkehr, die das StraBeninfrastruktursicherheitsmanagement, die Sicherheitsanforderungen in StraBentunneln sowie die Zulassung zum Beruf des Güterkraftverkehrsunternehmers oder des Personenkraftverkehrsunternehmers (Kraftomnibusunternehmen) betreffen,
    d) mit Vorgaben zur Gewährleistung der Eisenbahnbetriebssicherheit,

e) mit Vorgaben zur Sicherheit im Seeverkehr betreffend Vorschriften der Europäischen Union für die Anerkennung von Schiffsüberprüfungs- und -besichtigungsorganisationen, die Haftung und Versicherung des Beförderers bei der Beförderung von Reisenden auf See, die Zulassung von Schiffsausrüstung, die Seesicherheitsuntersuchung, die Seeleute-Ausbildung, die Registrierung von Personen auf Fahrgastschiffen in der Seeschifffahrt sowie Vorschriften und Verfahrensregeln der Europäischen Union für das sichere Be- und Entladen von Massengutschiffen,

f) mit Vorgaben zur zivilen Luftverkehrssicherheit im Sinne der Abwehr von Gefahren für die betriebliche und technische Sicherheit und im Sinne der Flugsicherung,

g) mit Vorgaben zur sicheren Beförderung gefährlicher Güter auf der StraBe, per Eisenbahn und per Binnenschiff,

h) mit Vorgaben zum Umweltschutz,

i) mit Vorgaben zum Strahlenschutz und zur kerntechnischen Sicherheit,

j) zur Förderung der Nutzung von Energie aus erneuerbaren Quellen und der Energieeffizienz,

k) zur Lebensmittel- und Futtermittelsicherheit, zur ökologischen Produktion und zur Kennzeichnung von ökologischen Erzeugnissen, zum Schutz geografischer Angaben für Agrarerzeugnisse und Lebensmittel einschlieBlich Wein, aromatisierter Weinerzeugnisse und Spirituosen sowie garantiert traditioneller Spezialitäten, zum Inverkehrbringen und Verwenden von Pflanzenschutzmitteln sowie zur Tiergesundheit und zum Tierschutz, soweit sie den Schutz von landwirtschaftlichen Nutztieren, den Schutz von Tieren zum Zeitpunkt der Tötung, die Haltung von Wildtieren in Zoos, den Schutz der für wissenschaftliche Zwecke verwendeten Tiere sowie den Transport von Tieren und die damit zusammenhängenden Vorgänge betreffen,

l) zu Qualitäts- und Sicherheitsstandards für Organe und Substanzen menschlichen Ursprungs, Human- und Tierarzneimittel, Medizinprodukte sowie die grenzüberschreitende Patientenversorgung,

m) zur Herstellung, zur Aufmachung und zum Verkauf von Tabakerzeugnissen und verwandten Erzeugnissen,

n) zur Regelung der Verbraucherrechte und des Verbraucherschutzes im Zusammenhang mit Verträgen zwischen Unternehmern und Verbrauchern sowie zum Schutz von Verbrauchern im Bereich der Zahlungskonten und Finanzdienstleistungen, bei Preisangaben sowie vor unlauteren geschäftlichen Handlungen,

o) zum Schutz der Privatsphäre in der elektronischen Kommunikation, zum Schutz der Vertraulichkeit der Kommunikation, zum Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation, zum Schutz der Privatsphäre der Endeinrichtungen von Nutzern und von in diesen Endeinrichtungen gespeicherten Informationen, zum Schutz vor unzumutbaren Belästigungen durch Werbung mittels Telefonanrufen, automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post sowie über die Rufnummernanzeige und -unterdrückung und zur Aufnahme in Teilnehmerverzeichnisse,

p) zum Schutz personenbezogener Daten im Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz- Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) gemäß deren Artikel 2,

q) zur Sicherheit in der Informationstechnik im Sinne des § 2 Absatz 2 des BSI-Gesetzes von Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes,

r) zur Regelung der Rechte von Aktionären von Aktiengesellschaften,

s) zur Abschlussprüfung bei Unternehmen von öffentlichem Interesse nach § 316a Satz 2 des Handelsgesetzbuchs,

t) zur Rechnungslegung einschließlich der Buchführung von Unternehmen, die kapitalmarktorientiert im Sinne des § 264d des Handelsgesetzbuchs sind, von Kreditinstituten im Sinne des § 340 Absatz 1 des Handelsgesetzbuchs, Finanzdienstleistungsinstituten im Sinne des § 340 Absatz 4 Satz 1 des Handelsgesetzbuchs, Wertpapierinstituten im Sinne des § 340 Absatz 4a Satz 1 des Handelsgesetzbuchs, Instituten im Sinne des § 340 Absatz 5 Satz 1 des Handelsgesetzbuchs, Versicherungsunternehmen im Sinne des § 341 Absatz 1 des Handelsgesetzbuchs und Pensionsfonds im Sinne des § 341 Absatz 4 Satz 1 des Handelsgesetzbuchs,

4. Verstöße gegen bundesrechtlich und einheitlich geltende Regelungen für Auftraggeber zum Verfahren der Vergabe von öffentlichen Aufträgen und Konzessionen und zum Rechtsschutz in diesen Verfahren ab Erreichen der jeweils maßgeblichen EU-Schwellenwerte,

5. VerstöBe, die von § 4d Absatz 1 Satz 1 des Finanzdienstleistungsaufsichtsgesetzes erfasst sind, soweit sich nicht aus § 4 Absatz 1 Satz 1 etwas anderes ergibt,

6. VerstöBe gegen für Körperschaften und Personenhandelsgesellschaften geltende steuerliche Rechtsnormen,

7. VerstöBe in Form von Vereinbarungen, die darauf abzielen, sich in missbräuchlicher Weise einen steuerlichen Vorteil zu verschaffen, der dem Ziel oder dem Zweck des für Körperschaften und Personenhandelsgesellschaften geltenden Steuerrechts zuwiderläuft,

8. VerstöBe gegen die Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union sowie VerstöBe gegen die in § 81 Absatz 2 Nummer 1, 2 Buchstabe a und Nummer 5 sowie Absatz 3 des Gesetzes gegen Wettbewerbsbeschränkungen genannten Rechtsvorschriften,

9. VerstöBe gegen Vorschriften der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1),

10 .ÄuBerungen von Beamtinnen und Beamten, die einen VerstoB gegen die Pflicht zur Verfassungstreue darstellen.

(2) Dieses Gesetz gilt auBerdem für die Meldung und Offenlegung von Informationen über

1. VerstöBe gegen den Schutz der finanziellen Interessen der Europäischen Union im Sinne des Artikels 325 des Vertrags über die Arbeitsweise der Europäischen Union und

2. VerstöBe gegen Binnenmarktvorschriften im Sinne des Artikels 26 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union, einschlieBlich über Absatz 1 Nummer 8 hinausgehender Vorschriften der Europäischen Union über Wettbewerb und staatliche Beihilfen.

ANNEX 6 - GIBRALTAR

The Speak Up Policy is amended for those working in and protected by the laws of Gibraltar as the following sentence under paragraphs 1.1 is not compliant with such legislation:

“1.1 However, this Speak Up Policy should not be used to:…. Make inaccurate, malicious or vexatious allegations. If an employee makes such complaints, and particularly if they persist with making them, disciplinary action may be taken against them.”

Such clauses are replaced as follows:

“1.1 However, this Speak Up Policy should not be used to: make false allegations maliciously. If an employee makes such complaints, and particularly if they persist with making them, disciplinary action may be taken against them.”

ANNEX 7 - ISRAEL

The Speak Up Policy is clarified for those working in and protected by the laws of Israel, as follows:

- It should be clarified that any complaint regarding sexual harassment in the context of employment relations, or any complaint about harm of any kind originating from sexual harassment, or from a complaint or lawsuit filed regarding sexual harassment, should be submitted to the officer in charge of this matter at Playtech.
- These complaints will be addressed and examined in accordance with any policy operated by Playtech in respect of sexual harassment.

ANNEX 8 - ITALY

The Speak Up Policy is amended for those working in and protected by the laws of Italy, by adding in the relevant paragraphs provided below:

2.1. How to Raise a Concern

An external reporting channel has been set up at the National Anti-Corruption Authority (ANAC). You can make a report to this channel in any of the following cases:

(a) the above reporting channels do not comply with the provisions of this Speak Up Policy regarding the confidentiality of the processed information and data;

(b) the reporting person has already made a report under the above and the report has not been followed up;

(c) the reporting person has reasonable grounds to believe that a report made under the above would not be effectively followed up, or that the report may lead to retaliation; or

(d) the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

Guidance for using the ANAC external reporting channel can be found at https://www.anticorruzione.it/-/whistleblowing.

2.2. What Happens When a Concern is Raised

1. Personnel will receive an initial response to acknowledge receipt of their concern. From there, the Chief Compliance Officer, General Counsel or their appointed investigating lead will provide regular feedback and updates on the progress of the investigation into their concern until the matter has been resolved. If you contact the external Speak Up Line, you will receive a unique case number, which you can use to check the status of your concern and/or add additional information. A feedback will always be provided within the 3 months following the “acknowledge receipt” of the concern (or following the 7th day after the concern is raised, if earlier).
2. Disciplinary action may also be taken against the reporting person when such person commits a crime in order to obtain the information related to the report; or in relation to any misconducts that are not strictly necessary for the report.

2.3. Confidentiality and Anonymity

For those reasons outlined in the Speak Up Policy, Playtech encourages Personnel to include their name in any disclosures. Playtech will only make the employee's name known to those people who need to know it in order to investigate the allegation, or otherwise as required by law. Except for such cases, the identity of the reporting employee will not be disclosed, unless the latter consents to such disclosure.

ANNEX 9 - LATVIA

The Speak Up Policy is amended for those working in and protected by the laws of Latvia as a number of paragraphs are not compliant with such legislation.

Such clauses are replaced as follows:

1. **Chapter "About this policy" subsection "Application of this policy" Second sentence:**

   "This Policy applies to all persons working for, or on behalf of, Playtech in any capacity, including employees at all levels, shareholders, directors, officers, agency workers, seconded workers, volunteers, interns, and where appropriate, agents, contractors, external consultants, third-party representatives and business partners, sponsors, persons establishing legal relations related to the fulfilment of work duties, or any other persons associated with Playtech, wherever located. "

2. **1.1. Speaking up, or whistleblowing, is raising genuine concerns about suspected unsafe, unethical or unlawful behaviour at work. This may include (but is not limited to):**

Criminal activity, an administrative offence, or another violation of legal norms (act or omission), including action which is contrary to the purpose of the legal act, and also a violation of the binding ethical or professional standards;

3. **1.1. last sentence:**

   If Personnel are uncertain whether something is within the scope of this Policy, they should seek advice from one of the individuals listed in paragraph 2.1.

4. **2.1. Playtech hopes that in many cases Personnel will be able to find a solution by discussing the concern with the line manager or local P&C or business unit representative.**

   The line manager may be able to agree a way of resolving the concern quickly and effectively. However, if Personnel consider to raise concern according to the Speak Up Policy, all concerns shall be raised in person or the matter in writing and should state that they are raising a concern under the Speak Up Policy.

   Personnel depending on the situation may choose one of the reporting mechanisms: reports at his local subsidiary directly or centrally at the Playtech parent company.

   All concerns under this Speak Up Policy may be raised locally or centrally at the option of Personnel by using the local channel:

   - For local reporting SpeakUp.Latvia@playtech.com
   - For central reporting to the confidential external 'Speak Up Line'

   We would hope that you feel able to report internally to one of the contacts above within Playtech. However, if the nature of the matter is such that you cannot raise it with any of the contacts identified above or, if you have followed the internal channels listed above and you still have concerns, you can contact our confidential external 'Speak Up Line'. The Speak Up Line is an independent external hotline provided by Convercent for Playtech which allows Personnel across the Playtech Group to raise concerns in their native language via telephone or via a secure web portal. From there, your report will be passed to Playtech and be dealt with in accordance with this Speak Up Policy.

   The concern may be raised also by providing information publicly if at least one of the following conditions is in effect:

   - The Personnel is not informed of the course of examination of his or her report within the time period specified in Section 2.2.of this Policy;
   - The violation indicated in the Personnel report is not eliminated for a lengthy period without any objective reason;

- Personnel has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest; or
- Personnel has reasonable grounds to believe that, in using the internal reporting mechanism adverse effects will be caused, the violation will be hidden or will not be eliminated.

5. 2.2. What happens when a concern is raised

1. When a person raises a concern internally, the details depending on the reporting channel used by the person are channeled to:
   (a) The local responsible person to investigate further if the report has been submitted locally; or
   (b) The Chief Compliance Officer and General Counsel to investigate further, if the report has been submitted to the Chief Compliance Officer, General Counsel or Global Director of People & Culture or by using the 'Speak Up Line'.
2. Where appropriate, the responsible person may assign a team to conduct an investigation to gather and establish relevant facts relating to the matter. This may include the appointment of an independent, external legal advisor to support the review. Personnel may also be asked to provide further information, or answer questions about their concern, if required.
3. The person raising the concern will receive an initial response to acknowledge receipt of their concern within 7 (seven) days after submission of the report. From there, the responsible person or their appointed investigating lead will provide regular feedback and updates on the progress of the investigation into their concern until the matter has been resolved. This includes, but is not limited to:
   - Sending a decision on whether or not to recognise a report as a report within the meaning of this Policy;
   - Sending information of the progress of the investigation of the person's report not later than within two months from the day when the submission of the person has been recognised to be a report within the matter of this Policy;
   - Sending information of the facts established and the decision taken or activities performed shall be sent to the Personnel after examination of the Personnel's report has been completed.

   If you contact the external Speak Up Line, you will receive a unique case number, which you can use to check the status of your concern and/or add additional information.
4. Playtech will use its best efforts to finalise the investigation process as soon as possible, but the duration of an investigation can vary depending on the complexity and severity of the concern raised. Playtech aims to resolve all matters, and to provide feedback to the Personnel, as soon as reasonably possible following the report.
5. Following the investigation, the investigating lead will produce a written report on the matter containing the findings of the investigation, the reasoning behind the decision and recommendations to address the issue. The report may be shared with the senior management of the local subsidiary, Chair of the Audit and Risk Committee of the Board and with the Chief Executive and Chairman, if appropriate.
6. Once the relevant members of senior management have been informed and consulted without compromising any confidentiality, the Responsible person will implement the relevant actions required to resolve the matter, which could include disciplinary and/or other actions.
7. Where possible, the employee will be informed of the outcome of any investigations carried out and any actions taken, although confidentiality requirements may prevent this in some cases.
8. If, during examination of the report, there are suspicions of a violation in which the examination does not fall within the competence of Playtech, the report will be transferred for examination based on the jurisdiction and the Personnel will be informed thereof. If there is evidence of

criminal activity, the Responsible person may consult external legal counsel and may report to the relevant law enforcement authorities. Playtech will ensure that any internal investigation does not hinder a formal police investigation.

9. Not changed.
10. Not changed.

6. **2.3. Confidentiality and anonymity**

Playtech will treat all concerns and disclosures made under this Policy in a confidential and sensitive manner and will treat any information with respect. If a Personnel report has been recognised as a whistleblowers report within the meaning of this Policy after the submission, the personal data of its submitter will be pseudonymised. Pseudonymisation need not be performed if the Personnel has already disclosed his or her identity to the competent authority in a similar case or the whistle has been blown in public, or the person has disclosed his or her identity publicly.

Anonymous whistleblowing is not accepted by the local laws. For this reason, Playtech encourages Personnel to include their name in any disclosures. Playtech will only make the Personnel's name known to those people who need to know it in order to investigate the allegation or otherwise as required by law.

It is possible that the investigation process may reveal the source of the information.

Alternatively, the employee making the disclosure may need to provide a statement as part of the evidence required. In the event such disclosure is necessary, this will be discussed with the Personnel beforehand, and the information will only be communicated with the investigating lead charged with looking into and resolving the concern and protected according to the applicable data protection regulations.

7. **2.4. Protection and support for speaking up, first sentence:**

It is understandable that Personnel who speak up may be concerned about possible repercussions and/or retaliation against them, their family members or related persons. If Personnel believe that they have suffered detrimental treatment, they should inform the local management, Chief Compliance Officer, General Counsel, Global Director of People and Culture or the Speak Up line immediately.

ANNEX 10 - PERU

This Annex includes the applicable Peruvian regulation, which is the SBS Resolution # 1695-2026, Anti-Money Laundering Rules for Gambling Services.

1. For the fulfilment of this policy, any employee in Peru could directly contact the local Compliance Officer.
2. Each employee is committed to attend the respective training program with the scope as detailed within the Peruvian regulation.
3. Each employee is committed to present any personal and economic information duly updated to Playtech through the local P&C department.
4. For any unusual activity, the local Compliance Officer will start an investigation to proceed in case such activity could qualify as suspicious.
5. Suspicious activity found out by the local Compliance Officer shall be reported to the Financial Intelligence Unit within a Suspicious Activity Report called ROS.
6. In annex 4 of the SBS Resolution # 1695-2026 any employee will find alert activities to be aware of any risk involving Playtech's local industry.
7. For the fulfilment of the anti-money laundering system, each employee is committed to follow the internal Code of Conduct and the Anti-money laundering Manual.
8. Regarding the Data Protection clause in 2.6 of this policy, the Law # 29733 and its complimentary regulation will apply.

ANNEX 11 - ROMANIA

The Speak Up Policy is amended for those working in and protected by the laws of Romania, as paragraphs **2 of the Introductory part, Clause 1.1, Clause 2.1, Clause 2.2., Clause 2.4 and Clause 2.5.** are not compliant or should be completed in accordance with such legislation.

Such clauses are replaced and completed as follows:

A. In the introductory part of the Speak Up Policy, the Section relating to **Application of this Policy, paragraph 2** shall have the following content:

"This Policy applies to:

e) workers or former workers;

e) persons having self-employed status;

e) interns, volunteers or job applicants;

e) any shareholders and persons belonging to the administrative, management or supervisory body of the company, including non-executive membersany partners, suppliers, vendors, or other alike, including those attempting to enter into a business relationship with the company, as well as any person working under the supervision and direction of such."

B. **Section 1 Speaking Up, Clause 1.1., What is speaking up is completed as follows:**

"*Speaking up or whistleblowing also includes raising genuine concerns about breaches of law, meaning any infringements, which may also involve criminal activity, of EU laws, irrespective of the matter, which can cause harm to the laws from areas such as: public procurement; services, products and financial markets, and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiological protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; privacy and personal data protection and network and information systems security; infringements affecting the financial interests of the European Union; infringements relating to the internal market etc.*"

The law applicable to Whistleblowing in Romania is Law no. 361/2022, adopted in light of the Directive (EU) 2019/1937 ("the Whistleblowing Directive"). This policy describes the personnel's rights and how the personnel can exercise them. "

C. After Clause 1.1. What is speaking up, a new Clause 1.2. Main Responsibilities is added, with the following content:

"The Company is responsible for putting in place an internal reporting channel, for adequately managing the concerns raised and to ensure their investigation as soon as practicable.

The Company and the Appointed Person has the obligation to not disclose the whistleblower's identity, nor the information that would allow his direct or indirect identification, except in the case where he has his express consent or disclosure is mandatory by law. The Company should ensure that whistle-blowers are not subject to retaliation measures.

Reporting on breaches of the law is mainly done through the existing internal reporting channels. However, a whistleblower can choose between the internal reporting channel (directly to the Company) and the external reporting channel (to the competent authorities, in Romania - the National Agency for Integrity)."

D. Clause 2.1, How to raise a concern shall have the following content:

"*The report can be made in writing, on paper or electronically, via phone calls or other voice mail systems and at the request of the whistleblower - via face-to-face meeting.*

If made in writing, the concern raised should have attached evidence and documents which may facilitate subsequently the carrying out of the investigation of the raised concern.

*Personnel will be able to raise any concerns with the following person: Mi**haela Brundusa Mindescu, People & Culture Manager** (the "**Appointed Person**"). Personnel should state that they are raising a concern under the Speak Up Policy.*

We would hope that you feel able to report internally to the Appointed Person within Playtech. However, if the nature of the matter is such that you cannot raise it with any of the contacts identified above or, if you have followed the internal channel listed above and you still have concerns, you can contact our confidential external 'Speak Up Line'. The Speak Up Line is an independent external hotline provided by OneTurst for Playtech which allows Personnel across the Playtech group to raise concerns in their native language via telephone or via a secure web portal. From there, your report will be passed to Playtech and be dealt with in accordance with this Speak Up Policy."

The concern may be also raised anonymously. However, anonymously raising concerns may render the investigation more difficult and may impede certain measures from being taken.

E. <u>After Section 2.1,</u> it will be added a new section**<u>, Section 2.1.[1] - What can be reported</u>**

"*Raising a concern can be initiated in cases where the whistleblower obtains information within the framework of a professional relationship/activity within Playtech and has reasonable grounds to appreciate that there is a breach of law. Reasonable grounds means that considering the circumstances and information available upon the moment of the reporting, the whistleblower considers the concern raised as being true.*"

F. <u>Section 2.2., What happens when a concern is raised, shall have the following content:</u>

1. *Where appropriate, the Company may assign, on a confidential basis, a team to conduct an investigation to gather and establish relevant facts relating to the matter. This may include the appointment of an independent, external legal advisor to support the review. Personnel may also be asked to provide further information, or answer questions about their concern, if required.*
2. *Personnel will receive an initial response to acknowledge receipt of their concern within 7 (seven) days from receipt. From there, the Appointed Person or the appointed investigating lead will provide regular feedback and updates on the progress of the investigation into their concern until the matter has been resolved. If you contact the external Speak Up Line, you will receive a unique case number, which you can use to check the status of your concern and/or add additional information.*
3. *Playtech will use its best efforts to finalise the investigation process as soon as possible, but the duration of an investigation can vary depending on the complexity and severity of the concern raised. Analysing and resolving the complaint shall take as a rule, a maximum of 3 (three) months from the acknowledgment of receipt or, if no acknowledgement was sent, from the expiry of the 7-day period from receipt; if the case, the Company shall send follow-up notices on the status of the investigation and related measures taken, subject to the circumstances. Playtech aims to resolve all matters, and to provide feedback to the whistleblower, as soon as reasonably possible following the report.*
4. *Following the investigation, the investigating lead will produce a written report on the matter containing the findings of the investigation, the reasoning behind the decision and recommendations to address the issue. The report may be shared on a confidential basis with the Chair of the Audit and Risk Committee of the Board and with the Chief Executive and Chairman, if appropriate*
5. *Once the relevant members of senior management have been informed and consulted without compromising any confidentiality, the Company will implement the relevant actions required to resolve the matter, which could include disciplinary and/or other actions.*
6. *The employee will be informed of any way Playtech proposes to resolve the matter after the investigation is carried out.*

7. *If there is evidence of criminal activity, the Company may report to the relevant law enforcement authorities. Playtech will ensure that any internal investigation does not hinder a formal police investigation.*
8. *Playtech will make every effort to address Personnel' concerns confidentially, fairly and professionally.*
9. *If Playtech concludes that Personnel have made false allegations maliciously, Personnel may be subject to disciplinary action. Also, as per Romanian Law, reporting complaints on breaches knowing them to be untrue represents an offence and may be punished by a fine if the offence has not been committed under such conditions to be considered a criminal offence.*

Section 2. 4. <u>Protection and support for Speaking Up</u> shall be completed with the following paragraphs:

As per the law, besides the whistleblower, the following persons are protected from retaliation or other negative measures:

c) persons having a certain relationships with the whistleblower (such as spouse, friends, etc.);

c) individuals who assist the whistleblower in the reporting process in a professional context (so-called "facilitators"); and

c) legal persons instructed by the whistleblower or for whom the whistleblower works or with whom the whistleblower has another professional relationship.

"Please consider that, in addition to the information provided based on this Policy, the Romanian competent authority may offer further information and independent advice, which can be free of charge/freely accessed in respect of concerns regarding the available procedures and challenge, as well as protection against retaliation and your rights. The contact information can be found here: Agentia Nationala de Integritate*."*

Section 2.5 External Disclosures shall have the following content:

The aim of this Policy is to provide an internal mechanism for reporting, investigating, and remedying any wrongdoing in the workplace. The law recognises that in some circumstances it may be appropriate for Personnel to report concerns to an external body such as a regulator; however, Playtech strongly encourages Personnel to seek advice before reporting a concern to external organisations.

Concerns may relate to staff as well as the actions of a third party, such as a customer, supplier, or service provider. In some circumstances, the law will protect Personnel if raising a matter with the third party directly. However, Playtech encourages Personnel to report such concerns internally first. Personnel should contact the Appointed Person, if they're unsure whether or not they wish to raise a concern under this policy or make an external disclosure.

ANNEX 12 - SPAIN

The Speak Up Policy is amended for those working in and protected by the laws of Spain and has been drafted taking into account the country-specific requirements of the Spanish Whistleblowing Act 2/2023 (hereinafter the "**LPID**"). For whistleblowers located in Spain and covered by the LPID, this appendix shall prevail over the main body of the Speak Up Policy.

Playtech understands that you, as data subject, may have concerns about your privacy and how your personal data is processed in the context of reporting misconduct. Employees interacting with Playtech can get access to full information on how Playtech collects and processes their personal information through Playtech ' Privacy Policy, with which they should be familiar, the latest version of which is available at the following webpage: https://playtech.my.onetrust.com.

Under the LPID, Playtech is the data controller for the personal data processed within the reporting scheme, and the purposes of processing your personal information are the implementation, management, and verification of the reporting scheme, as well as adopting the corrective measures that the results of an investigation may identify as necessary. If the implementation of the scheme is merely voluntary or convenient or if it relates to a public disclosure, the legal basis for processing your personal information will be the fulfilment of a public interest task endorsed by the LPID (Article 6.1.e) of the GDPR). If, due to the size of Playtech and/or other circumstances, the scheme becomes legally mandatory, then the legal basis for processing your personal information would be the compliance with the law (Article 6.1.c) of the GDPR).

Please note that the LPID only covers whistleblowing report acts or omissions which may constitute breaches of EU law, or which may constitute serious or very serious criminal or administrative offences. Because of it, Playtech will only process personal data for whistleblowing purposes in those circumstances, always only within the scope of Article 2 of the LPID .

Playtech shall not disclose the identity of a reporting person to the people to which the report referred to nor to third parties. Where Playtech considers it must reveal that information in accordance with the LPID, including to the courts, the public prosecutors, or the relevant law enforcement agencies in charge, in the context of a criminal, disciplinary or regulatory investigation, Playtech will try to give the person who made the report early warning of such disclosure(s), except if this could hamper the ongoing investigation or court procedures.

Notwithstanding the foregoing, you shall always keep in mind that several people may get access to your personal information, in accordance with the LPID. The list of these authorized individuals would include (a) the Chief Compliance Officer and the person effectively managing the investigation, if applicable, (b) the Global Head of HR or the body appointed to replace him/her, but this only when it could be necessary to adopt disciplinary measures against an employee, (c) the General Counsel, but this only when it could be necessary to adopt legal measures regarding the reported facts, (d) the data processor in charge, (e) the relevant Playtech's Data Protection Officer, and (f) other people whose intervention is essential to adopt corrective measures or to move forward with disciplinary or criminal law procedures.

Whenever a report is received, Personnel will receive an initial response to acknowledge receipt of their concern in no more than 7 natural days, and the report will be registered in the Information Management System. Once received, the people managing it will have to decide whether a formal investigation is opened or not, considering the facts reported and the circumstances of the case. This decision shall be made as soon as possible and, in any event, within three (3) months from the date on which the report had been received. Whenever the decision has been negative or has not been made within that three-month period, all personal data contained in the report will be deleted.

You, as a data subject, will always be entitled to exercise your rights of access, rectification, erasure, objection to and limitation of the processing and, if applicable, portability, in accordance with Articles 15 to 22 of the GDPR. You can also file a complaint in front of the relevant data protection regulator.

No special category data (e.g., ethnic origin, religious belief, sexual orientation), that is unnecessary for the purposes of the reporting scheme, or false data, will be collected nor processed within the context of this reporting scheme. If collected by accident or error, such data will be promptly deleted.

ANNEX 13 - SWEDEN

QUICKSPIN AB

The Speak Up Policy is amended for those working in Quickspin AB and that are protected by the laws of Sweden, as paragraphs 1.1, 2.1, 2.2 and 2.5 are not compliant with such legislation.

Such clauses are replaced as follows:

Clause 1.1 (What is speaking up?) is replaced by the following:

What can I raise a concern about?

Speaking up, or whistleblowing, is raising genuine concerns about suspected unsafe, unethical or unlawful behaviour at work. You do not need to have evidence of your suspicions to raise a concern, but all reports must be made in good faith, and you must have reasonable grounds to believe that the information about the misconduct is true.

Whistleblowing reports may only relate to suspected misconduct in a work-related context for which there is a public interest in disclosure or to suspected breaches of so-called Union law, i.e., EU law and its sources of law. This may include (but is not limited to):

(a) Criminal activity;

(b) Failure to comply with any legal obligation or regulatory requirement;

(c) Danger to health, safety and/or employee safeguarding concerns under Playtech's Wellbeing Policy;

(d) Damage to the environment;

(e) Human rights and/or modern slavery breaches contrary to Playtech's Human Rights Policy;

(f) Bribery contrary to Playtech's Anti-Bribery and Corruption Policy;

(g) Facilitation of tax evasion contrary to Playtech's Anti-Facilitation of Tax Evasion Policy;

(h) Financial fraud or mismanagement;

(i) Negligence;

(j) Unethical behaviour contrary to Playtech's Business Ethics Policy;

(k) Money laundering contrary to Playtech's Anti-Money Laundering and Counter-Terrorist Financing Policy;

(l) Conduct likely to damage Playtech's reputation;

(m) Unauthorized disclosure of confidential information or other data breaches contrary to Playtech's Data Protection and Privacy Policy;

(n) Bullying or sexual harassment;

(o) or The deliberate concealment of any of the above.

This Speak Up Policy should not be used to:

Question financial or business decisions taken by Playtech;

(a) Raise concerns relating to an employee's personal circumstances, such as the terms of their contract. In those cases, the employee should use the Grievance Procedure, which can be found in the employee handbook and/or by asking the People & Cultures ('P&C') Department for the procedure;

(b) Reopen matters that have already been addressed under Playtech's harassment, disciplinary or other procedures; or

(c) Make inaccurate, malicious or vexatious allegations. If an employee makes such complaints, and particularly if they persist with making them, disciplinary action may be taken against them

If you are uncertain whether something is within the scope of the Speak Up Policy, you seek advice from the Compliance group.

Who may raise a concern?

To raise a concern by blowing the whistle, you must fall into one of the following categories of persons:

(a) Workers.

(b) Volunteers.

(c) Trainees.

(d) Temporary staff or persons who are otherwise available to the Company for the performance of work.

(e) Self-employed persons or consultants.

(f) Persons in the administrative, management or supervisory body of the Company.

(g) Shareholders active in the Company.

If you do not belong to any of the above categories of persons, you can instead turn to a line manager whom you trust or report using the external reporting channels of the competent authorities. If you report even though you do not belong to any of the above categories of persons, you will be informed about this and, if appropriate, referred to another suitable reporting channel.

Clause 2.1 (How to Raise a Concern) is replaced by the following:

You have the right to raise a concern in writing or orally. To raise a concern, you may either use our external Speak Up Line or contact designated persons.

1. Speak Up Line

   The Speak Up Line is an independent external hotline provided by Convercent which allows you to raise concerns in your native language. You can submit a report in the Speak Up Line in writing via a secure web portal or orally by telephone.

2. Contact designated persons

   Contact the Compliance group.

You also have the right to raise concerns orally by requesting a face-to-face meeting. We will offer you a meeting within one week of the receipt of your request.

If you choose to raise concerns orally, the report will be documented by means of a recording, if you agree to this, or by taking minutes. A recorded report may also be documented by a transcript of the recording. In this case, you will be given the opportunity to check, correct and sign the protocol or transcript.

Clause 2.2 (What Happens When a Concern is Raised) is replaced by the following:

1. Once you have raised a concern, it will be channeled to the Chief Compliance Officer and General Counsel. You will receive an acknowledgement that your report has been received within seven days, unless you have declined such acknowledgement or there is reason to believe that an acknowledgement could reveal your identity.
2. Where appropriate, the Chief Compliance Officer and General Counsel may assign a team to conduct an investigation to gather and establish relevant facts relating to the matter. This may include the appointment of an independent, external legal advisor to support the review. You may also be asked to provide further information, or answer questions about your concern, if required.

3. Within three months from sending you an acknowledgement of receipt of your report, you will, as far as possible, be provided with feedback on the investigative measures taken. If you have not received an acknowledgement of receipt, you will instead be provided with feedback within seven days of us receiving your report. If you raise concerns via the external Speak Up Line, you will also receive a unique case number, which you can use to check the status of your concern and/or add additional information.
4. We will use our best efforts to finalise the investigation process as soon as possible, but the duration of an investigation can vary depending on the complexity and severity of the concern raised. When the investigation is closed, you will receive a notification. The notification will not necessarily contain the outcome of the investigation. This is because such information may be sensitive to share.
5. Following the investigation, the investigating lead will produce a written report on the matter containing the findings of the investigation, the reasoning behind the decision and recommendations to address the issue. The report may be shared with the Chair of the Audit and Risk Committee of the Board and with the Chief Executive and Chairman, if appropriate.
6. Once the relevant members of senior management have been informed and consulted without compromising any confidentiality, the Chief Compliance Officer and General Counsel will implement the relevant actions required to resolve the matter, which could include disciplinary and/or other actions.
7. Where possible, you will be informed of the outcome of any investigations conducted and any actions taken, although confidentiality requirements may prevent this in some cases.
8. If there is evidence of criminal activity, the Chief Compliance Officer and General Counsel may consult external legal counsel and may report to the relevant law enforcement authorities. We will ensure that any internal investigation does not hinder a formal police investigation.
9. We will make every effort to address your concerns confidentially, fairly, and professionally. If you are not happy with the way in which a concern has been handled, you can contact any of the contacts listed in the section How to Raise a Concern.
10. If we conclude that you have made false allegations maliciously, you may be subject to disciplinary action.

Clause 2.5 (External Disclosures) is replaced by the following:

Reporting to competent authorities' external whistleblowing channels

If you do not want to report using any of the channels described in Clause 2.1, you have the possibility to report misconduct to one of the external whistleblowing channels established by competent authorities. These are tasked with receiving, investigating, and providing feedback on reports of misconduct in various designated areas of responsibility.

If you want to submit a report to an external whistleblowing channel, you should first contact the competent authority responsible for the relevant area. A list of competent authorities, their responsibilities and contact details of their external whistleblowing channels can be found here. Via the external reporting channels, you have the right to report in writing, orally and by requesting a face-to-face meeting.

Freedom to collect and disclose information

The Swedish Freedom of the Press Act (Sw. *tryckfrihetsförordningen*) and the Swedish Fundamental Law on Freedom of Expression (Sw. *yttrandefrihetsgrundlagen*) provide for the right to submit information for publication in certain media (freedom to disclose information) and the right to acquire information for the purpose of communicating it for publication in certain media (freedom to collect information). However, as we are a privately owned company, these freedoms are limited by, among other things, contractual obligations of confidentiality (secrecy obligations) and general principles of duty of loyalty in employment relationships in the private labour market.

MOBENGA AB AND VIDEOBET INTERACTIVE SWEDEN AB

The Speak Up Policy is amended for those working in Mobenga AB and Videobet Interactive Sweden AB, and that are protected by the laws of Sweden, as paragraph 1.1 is not compliant with such legislation.

Such clauses are replaced as follows:

Clause 1.1 (What is speaking up?) is replaced by the following:

Anyone within the Company may blow the whistle regarding (suspected) irregularities or crimes of a serious nature by an individual who is in a leading position or who is considered key personnel within the Company or within the Playtech Group. Such individuals include board members, persons in management, and other persons that act with a high degree of autonomous decision power and who has a strong influence in the Company or the Playtech Group.

Irregularities of a serious nature that may be reported are serious irregularities relating to accounting, internal accounting controls, auditing, anti-bribery, banking and financial crime, or other serious irregularities affecting the vital interests of the organisation or the life and health of individuals.

Examples of such irregularities are:

(a) Criminal activity;

(b) Failure to comply with any legal obligation or regulatory requirement;

(c) Danger to health, safety and/or employee safeguarding concerns under Playtech's Wellbeing Policy;

(d) Damage to the environment;

(e) Human rights and/or modern slavery breaches contrary to Playtech's Human Rights Policy;

(f) Bribery contrary to Playtech's Anti-Bribery and Corruption Policy;

(g) Facilitation of tax evasion contrary to Playtech's Anti-Facilitation of Tax Evasion Policy;

(h) Financial fraud or mismanagement;

(i) Negligence;

(j) Unethical behaviour contrary to Playtech's Business Ethics Policy;

(k) Money laundering contrary to Playtech's Anti-Money Laundering and Counter-Terrorist Financing Policy;

(l) Conduct likely to damage Playtech's reputation;

(m) Unauthorised disclosure of confidential information or other data breaches contrary to Playtech's Data Protection and Privacy Policy;

(n) Bullying or sexual harassment; or

(o) The deliberate concealment of any of the above.

If you want to speak up about other irregularities, you can instead turn to a line manager whom you trust or speak with the People & Culture department.

ANNEX 14 - UKRAINE

The Speak Up Policy is amended for those working in and protected by the laws of Ukraine as paragraphs 1.1, 2.1, 2.2, 2.3, 2.4 are not compliant with such legislation.

In **paragraph 1.1.** the sentence "*the deliberate concealment of any of the above*" shall be deleted. Under art.9 of Law of Ukraine "*On Citizens' Appeals" no one may be forced to file a personal or to sign a collective appeal or to participate in campaigns for supporting the appeals of other persons or organisations.*"

Due to the requirements of art.5 of Law of Ukraine "On Citizens' Appeals" the **paragraph 2.1.** shall be added "*an appeal must contain the surname, given name and patronymic, place of residence of a citizen, indicate the essence of the issue, observation, proposal, application or complaint, request or demand. A written appeal must be signed by an applicant (applicants) with the indication of the date. An electronic appeal must also contain the e-mail address to which the applicant may receive a response or information on other means of communication with him/her. An appeal executed without compliance with these requirements shall be returned to the applicant with the relevant explanations no later than within ten days after the date of receiving it*".

Due to the requirements of art.20 of Law of Ukraine "On Citizens' Appeals" the **subparagraph 4 of paragraph 2.2.** shall be replaced for "*appeals shall be considered and resolved within no more than one month after receiving them, and appeals requiring no additional study – immediately, but no later than fifteen days after the date of their receipt. If it is impossible to resolve the issues raised in the appeal within one month, the head of enterprise or his/her deputy shall set the necessary deadline for considering it, whereof a person who has filed the appeal shall be notified. In this case, the total period of resolving the issues raised in the appeal may not exceed forty-five days*".

Due to the requirements of art.15 of Law of Ukraine "On Citizens' Appeals" the **subparagraph 7 of paragraph 2.2.** shall be added "*a decision to deny satisfaction of the demands set forth in an application (motion) shall be brought to the notice of the citizen in writing with reference to the Law and stating the reasons for refusal, as well as with an explanation of the procedure for appealing against the made decision*".

Due to the requirements of art.8 of the Law of Ukraine "On Citizens' Appeals" the **paragraph 2.3.** shall be replaced for "*a written appeal without the indication of the place of residence, not signed by an author (authors), as well as an appeal which makes it impossible to establish an author thereof, shall be recognised as anonymous and shall not be subject to consideration*".

Due to the requirements of art.26, 27 of the Law of Ukraine "On Citizens' Appeals" the **paragraph 2.4.** shall be added "*filing by a citizen of an appeal containing defamation and insults, discrediting heads and other officials of enterprises, institutions and organizations irrespective of the form of ownership, calls to incite ethnic, racial, religious hatred and other actions, shall entail liability. Expenses incurred by enterprise, institution, organisation irrespective of the form of ownership, citizens' associations, media in connection with verifying the appeals containing deliberately false information may be recovered from a citizen under the judgment*".