THE NET-A-PORTER GROUP LIMITED

PRIVACY NOTICE
ON MANAGEMENT OF WHISTLEBLOWING REPORTS
(Last updated on 18/12/2023)

THE NET-A-PORTER GROUP LIMITED (hereinafter, for the sake of brevity, "**NAP**", "**Controller**" or "**Company**"), part of YOOX Net-A-Porter Group S.p.A., is committed to achieve a safe and ethical work environment implementing a policy of integrity, responsibility and mutual trust.
Therefore, pursuant to the current rules on personal data protection, including European Regulation 2016/679 ("General Data Protection Regulation") as incorporated post-Brexit (hereinafter "**UK GDPR**") and Data Protection Act 2018, as amended through The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and latter's updates, together with the current rules regulating protected reporting on wrongdoing, or "whistleblowing", in particular:

- Public Interest Disclosure Act 1998, amending the Employment Rights Act 1996;

NAP wishes to inform you that, by reason of your capacity as worker (employee or temporary worker), volunteer or intern, even unpaid, collaborator of NAP, employee of NAP's third party suppliers, shareholder, individual who holds administration, management, control, supervision or representation functions within NAP or NAP's parent company or even according to a collaborative relationship between you and NAP (hereinafter collectively referred to as "**you**", "**reporting person**" or "**whistleblower**"), you have the faculty to report suspected misconduct and dangers, which may imply breaches of UK laws and regulations (hereinafter "**report**" or "**reports**"), via telephone and/or confidential online reporting system (provided by Navex Global), utilizing the secure channels the Company specifically allocated for reporting also in anonymous mode, at your convenience. Encryption techniques are applied to ensure the confidentiality of the information.
Your personal data in relation to your reports will be processed by NAP only for the purpose of elaborating, investigating, verifying your reports and ultimately act according to the outcomes. Whereas if you expressed the decision to report anonymously, the information you provide will be addressed to NAP on an entirely confidential and anonymous basis.

1. Controller and Data Protection Officer

The Controller is THE NET-A-PORTER GROUP LIMITED of 1 The Village Offices, Westfield London, Ariel Way, London, W12 7GF, United Kingdom, part of YOOX Net-A-Porter Group S.p.A. company under the direction and coordination of Compagnie Financière Richemont S.A., with headquarters in via Morimondo 17, 20143 - Milan (MI), Italy, Tax Code and VAT no. 02050461207.
For any queries, questions or needs connected with the processing of your personal data, please write to NAP's headquarters indicated above (to the attention of Whistleblowing Committee) or to the Data Protection Officer ("DPO") designated by NAP by writing to "Data Protection Officer" c/o 1 The Village Offices, Westfield London, Ariel Way, London, W12 7GF, United Kingdom or YOOX Net-A-Porter Group S.p.A., via Morimondo n. 17, 20143 - Milan (MI), Italy, or eventually by sending an email to DPO@ynap.com.

2. Categories of personal data, purposes and legal basis of data processing

Unless you report anonymously, NAP may process the following categories of data:

a) your identification data such as name and surname, your contact details such as phone number and email account; your city, region and Country of residence, your post code;
b) your position within the Company (or your unrelatedness), e.g. your possible qualification as a consultant/employee of NAP, jointly with your job location and department;
c) personal data relating to you, such as technical data associated with the report, e.g. metadata expressing your acceptance of terms and conditions of the online reporting system, as well as your credentials specifically generated for every single report;
d) identification data of individuals or entities concerned in your report ("persons concerned");
e) the description of the reported breaches of UK laws and regulations as well as the description of the circumstances of the occurrence, including the place where the reported event occurred.

<u>The aforesaid data mentioned in points a), b), c), d) and e) will be processed solely for the following purposes</u>:

1) to ensure verification of the information on breaches;
2) to fulfil specific legal obligations related to the purposes of the report, aimed at preventing corruption phenomena and other criminal activities;
3) to manage any litigation, protect the rights of the Company and adopt crime-fighting measures.

Personal information collected may also be processed to ensure:

- the correct and complete management of the whistleblowing procedure in compliance with current relevant legislation;

- the necessary investigative activities aimed at verifying the truthfulness of the occurrence reported, as well as the adoption of consequent measures;
- the response to a request from judicial authority or similar authorities.

Legal basis:

- regarding purposes of points 1) and 2), processing is necessary for compliance with a legal obligation to which NAP is subject (UK GDPR art. 6.1 (c)), obligation introduced in particular via Public Interest Disclosure Act 1998;
- regarding purposes of point 3) as well as to verify compliance of the behaviors reported with the company Code of Conduct and adopt adequate prevention measures to ensure reporting person's own safety, and when the processing involves special categories of personal data, NAP may act according to legitimate interests (UK GDPR art. 6.1 (f)).

In order to start any disciplinary proceedings against the alleged author of the reported conduct, the identity of the reporting person may only be revealed with the latter's consent (legal basis for the communication of data).

3. Source of data

All data mentioned in paragraph 2. will be provided directly by reporting persons. Aforementioned data may also be collected from third parties during activities related to the management of the report.

4. Method of data processing and consequences of your refusal to supply data

Your personal data will be processed by NAP using IT and paper-based systems in accordance with the applicable personal data protection rules, protecting your confidentiality and rights by taking appropriate technical and organisational measures to ensure an adequate safety level.
Your refusal to supply your personal data for the purposes referred to in paragraph 2. above does not affect your faculty to report through the secure channels the Company specifically allocated.
Please check over Navex Global's Terms and Conditions when reporting online.
When reporting keep in mind that:

- providing protection to an anonymous whistleblower may be more difficult, since there will be no evidence linking the reporting person to the anonymous report;
- accurately managing an anonymous report may be more difficult, a report is most effective when as many information as possible is provided. It is suggested that whistleblowers share their identity and that circumstances of the occurrence are as much detailed as possible to maximize the effectiveness of the assessment and the investigative process.

5. Data storage

NAP will store the abovesaid data (paragraph 2.) for the period of time that is strictly necessary to achieve the purposes set out in paragraph 2. or, if applicable, as long as necessary to initiate and conclude sanctioning proceedings or to meet legal needs. After a storage time of two years of the day the conclusive outcome of the reporting procedure is communicated, all data will be irremediably erased or will be made completely and irreversibly anonymous, unless their further storage is requested by competent judicial or administrative authorities or police forces or is necessary in relation to a Court dispute or for NAP's defence of legal claims.

6. Data recipients

For the purposes set out in paragraph 2. above and in accordance with the principles of UK GDPR, your personal data may be communicated:

1) to persons designated and authorised by NAP to engage in personal data processing operations (workers or collaborators of NAP) that are strictly connected with the purposes set out in paragraph 2. above. In particular, data and information provided may be accessed, processed and used by NAP's Whistleblowing Committee;
2) to data Processors appointed by NAP, involved in the management of activities connected with the purposes set out in paragraph 2. above (in this case, the provider of the confidential online reporting system);
3) where necessary, NAP shares your information with the controlling company YOOX Net-A-Porter Group S.p.A. (in quality of appointed data Processor).

Your data may also be communicated, in accordance with the law, to competent authorities, including police forces and judicial and administrative authorities, in order to establish and pursue offences, to prevent and avoid public security risks, to allow NAP to establish, exercise or defend legal claims and for other reasons connected to the protection of third parties rights and freedoms.

7. Data transfer

Data and information you provide will be stored by NAP on its servers located in UK and EU. Therefore, your data could be transferred by NAP outside UK, but not outside the European Union/European Economic Area.

Data and information collected via confidential online reporting system will be stored also on databases located on servers hosted and operated by third party provider, in this case Navex Global is subject to obligations and restrictions imposed by UK GDPR Chapter V about transfers of personal data and Data protection act 2018 provisions about transfers of personal data (e.g. transfers on the basis of an adequacy decision like "Data Privacy Framework" to which Navex Global adhered and/or standard contractual clauses between the Controller and the Processor).
Your data will not be spread.

8. Rights of the data subject

According to UK GDPR Chapter III, data subjects may enforce, relating to their personal data, the right of access, rectification and the right to be forgotten, as well as the right to restriction and objection to processing.
However, abovesaid rights cannot be exercised on a request to the Controller nor lodging a complaint with a supervisory authority (UK GDPR art. 77) if the exercise of these rights could result in an effective and concrete prejudice to the confidentiality of the identity of the reporting person.
To enforce the aforesaid rights, data subjects may contact the DPO designated by NAP by writing to "Data Protection Officer" c/o 1 The Village Offices, Westfield London, Ariel Way, London, W12 7GF, United Kingdom or YOOX Net-A-Porter Group S.p.A., via Morimondo n. 17, 20143 - Milan (MI), Italy, or eventually by sending an email to DPO@ynap.com.
Data subjects may also contact the supervisory authority (in UK the Information Commissioner's Office ICO) asking for inspections on the compliance of the processing of their data.