UNiDAYS

legal.team@myunidays.com

Whistleblower Policy

Purpose

UNiDAYS is committed to conducting our business with honesty and integrity, and we expect all staff to maintain high standards in accordance with our Corporate Code of Conduct.

However, all organisations face the risk of wrongdoing from time to time. A culture of openness and accountability is essential to prevent such situations from occurring and to address them when they do occur. The aims of this policy are:

- to encourage **UNiDAYS** staff, colleagues and stakeholders to raise their concerns within the business and report suspected wrongdoing as soon as possible, in the knowledge that we aim to ensure that their concerns will be taken seriously and investigated as appropriate and that their confidentiality will be respected;
- to provide staff, colleagues and stakeholders with guidance as to how to raise those concerns;
- to reassure staff, colleagues and stakeholders that they should be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken; and
- to explain how we will deal with whistleblowing disclosures, and how we will protect and support eligible whistleblowers.

Scope

This policy can be accessed by **all persons working or who have worked for UNiDAYS** or on its behalf in any capacity, including employees at all levels, directors, officers, workers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, including any relatives, dependants, or spouses of the aforementioned, wherever located (referred to throughout this policy as "Protected Persons").

This policy does not form part of any staff or employee and worker's contract of employment, and we may amend it at any time. It sets out useful information and explains procedures. You might need to comply with those procedures so that you can access the protections that **UNiDAYS** may make available to you.

Policy Detail

Responsible Parties:

UNiDAYS has overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to concerns raised under this policy.

The VP of People/Whistleblowing Officer, the Global General Counsel and Chairman of the Board have day-to-day operational responsibility for this policy and must ensure that all managers and other staff who may deal with concerns or investigations under this policy receive regular and appropriate training.

UNiDAYS will review this policy at least annually to assess its effectiveness, identify areas for improvement, and ensure that it remains aligned with best practices and relevant regulations.

All staff, colleagues, employees and workers are responsible for the success of this policy and should ensure that they use it to disclose any suspected danger or wrongdoing. Staff, colleagues, employees and workers are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the VP of People/Whistleblowing Officer or the Global General Counsel.

Background:

Whistleblowing is the disclosure of information in relation to which you have reasonable grounds to suspect misconduct, or an improper state of affairs or circumstances, in relation to **UNiDAYS** or a related company. This may include:

- criminal activity;
- failure to comply with any legal obligation or regulatory requirements;
- bribery under our Anti-corruption and Bribery Policy;
- facilitating tax evasion;
- misconduct, or an improper state of affairs, in relation to **UNiDAYS'** tax affairs;
- conduct that represents a danger to the public or the financial system;
- miscarriages of justice;
- health and safety risks;

- damage to the environment;
- suspicion of human trafficking or modern slavery whether at **UNiDAYS**, by a vendor or a partner, contrary to our Business Partner Code of Conduct; or
- the deliberate concealment of any of the above matters.

Depending on your region, Whistleblowing is protected only if it constitutes a 'protected disclosure' and the disclosure must be a 'qualifying disclosure' (*see Defined Terms*).

A **whistleblower** is a person who raises a genuine concern relating to any of the above. If you have any genuine concerns related to suspected wrongdoing or danger affecting any of our activities (a **whistleblowing concern**) you should report it under this policy. Current and former Protected Persons may all be eligible whistleblowers.

Personal Work-Related Grievances:

Personal work-related grievances are generally **NOT** whistleblowing disclosures and this policy will not apply to those types of grievances.

A personal work-related grievance is any complaint, concern or dispute to do with your employment (or previous employment) with **UNiDAYS** which has implications for you personally only. For example, a personal work-related grievance might include:

- a conflict between you and another staff member;
- if you think you have been personally discriminated against, bullied or harassed; and/or
- any dissatisfaction about a decision relating to your employment (such as a decision about transfer or promotion, the terms of your employment, discipline or termination).

Please read our Grievance Procedure and Anti-harassment and Bullying Policy as appropriate for details of how to raise any personal work-related grievance concerns.

However, a personal work-related grievance might ALSO be a whistleblowing disclosure if it:

- doesn't relate solely to you and impacts a wider group;
- is about various types of unlawful conduct or conduct that is a danger to the public or the financial system; and/or
- qualifies as a whistleblowing concern in line with this policy.

If your personal work-related grievance is also a whistleblowing disclosure, then it will attract whistleblower protection, and you can use the

procedures set out below.

If you are uncertain whether something is within the scope of this policy you should seek advice from the VP of People/Whistleblowing Officer, the Global General Counsel, our Chairman of the Board or through our confidential external telephone hotline and reporting system EthicsPoint contact details for each can be found at the end of this policy.

Making A Whistleblowing Disclosure:

You can make a whistleblowing disclosure by contacting the following:

- VP of People/Whistleblowing Officer or the Global General Counsel;
- Our confidential external telephone hotline and reporting system EthicsPoint (see below);
- An Appropriate Regulatory Authority (*see Defined Terms*)
- Depending on your region, a Permitted External Official (*see Defined Terms*)

If the concern is about the VP of People/Whistleblowing Officer or the Global General Counsel, then our whistleblowing tool, supported by EthicsPoint, will direct the complaint to our Chairman of the Board or an external systems advocate.

If you intend to make a whistleblowing disclosure, we ask that you please include in your statement or email/letter: "I am seeking to make a whistleblowing disclosure."

You should also ensure that any email or correspondence that you send is marked Strictly Confidential. While it might seem obvious, this will help **UNiDAYS** to:

- identify your concern as a whistleblowing disclosure;
- act on your disclosure promptly; and
- trigger the protections that are available for whistleblowing disclosure.

You should keep a file note of any correspondence or discussions (including the date and time) for future reference.

Contact details are set out at the end of this policy.

Information to include:

If you make a whistleblowing disclosure, you should consider providing as many of the following details as possible, to assist **UNiDAYS** or an authority in determining the best course of action:

- the specific nature of the conduct or state of affairs that concerns you;

- the details of the person/s you think engaged or is engaging in any relevant conduct;
- when and where relevant events occurred (e.g. dates and times);
- details of anyone else aware of or involved in the conduct or events;
- details of anyone else who might be able to verify your disclosure;
- if you have done anything in response to the conduct or events;
- if you have any concerns about possibly being victimised, and if so by whom; and
- any supporting information (e.g. documents, file notes, emails, photographs).

Please state expressly whether you give the person you contact permission to disclose your identity to the investigator, so the investigator can contact you to obtain further information if required.

Confidentiality:

We hope that you will feel able to voice whistleblowing concerns openly under this policy; however, if you want to raise your concern anonymously or through a pseudonym, you are entitled to do so.

You should understand that sometimes, if you choose to make disclosures anonymously, this can make it more difficult to undertake a proper investigation – particularly if we cannot obtain further information. It also makes it harder to provide you with relevant protections.

If you choose to identify yourself when you make the disclosure, please note that the person you contact is legally required to keep your identity strictly confidential in accordance with applicable law. If **UNiDAYS** is aware of your identity, we will aim to work with you to protect your identity.

Whistleblowers who are concerned about possible reprisals if their identity is revealed should come forward to the VP of People/Whistleblowing Officer or the Global General Counsel, or one of the contact points listed at the end of this policy, and appropriate measures can then be taken to preserve confidentiality. If you are in any doubt, we encourage you to seek advice from our confidential counselling hotline or one of the confidential helplines provided by independent whistleblowing organisations listed at the end of this policy.

It is understandable that whistleblowers are sometimes worried about possible repercussions. We will support whistleblowers who raise genuine concerns under this policy, even if they turn out to be mistaken. You may be permitted or even required to disclose confidential company information or trade secrets if doing so is necessary to report your concern.

Whistleblowers will not suffer any detrimental treatment as a result of raising a concern – see the section on protection and support for whistleblowers, below.

To the extent that you provide personal information as part of a disclosure, which relates to you or any other individual(s), **UNiDAYS** will process this personal information in accordance with applicable data protection laws and the Whistleblowing Privacy Notice available below.

Investigation and Outcome:

Once you have raised a concern, we will carry out an initial assessment to determine whether your disclosure requires further investigation.

In some cases, we may appoint an investigator or team of investigators, including staff with relevant experience in investigations or specialist knowledge of the subject matter. The investigator(s) may make recommendations for change to enable us to minimise the risk of future wrongdoing.

If you have identified yourself to us, we will inform you of the outcome of our assessment, if doing so is in compliance with confidentiality requirements. If you have given us permission to disclose your identity to the investigator, then the investigator may contact you to obtain further information, and you may be asked to attend additional meetings for that purpose. We will aim to let you know once an investigation has been conducted. However, sometimes the need for confidentiality may prevent us from giving you specific details of the investigation or any disciplinary action taken as a result. You should treat any information about the investigation as confidential.

A formal investigation might involve third parties such as lawyers, accountants, HR consultants or specialist forensic investigators, who will:

- interview relevant witnesses;
- collect relevant documentary evidence;
- make a determination based on the evidence; and
- document the findings.

Depending on your region, the investigator determines whether the information in the whistleblowing disclosure is proven on the balance of probabilities. The 'balance of probabilities' test requires consideration of whether it is more likely than not that the alleged conduct has occurred.

If the whistleblowing disclosures are proven, the investigator will report the outcome of the investigation to the appropriate decision-maker for further action (subject to any concerns about revealing your identity).

If the whistleblowing disclosures are not proven, but there is evidence of other inappropriate conduct, the matter might be referred to the People Team. For example, there may be evidence of a breach of **UNiDAYS** company policy or violation of our Corporate Code of Conduct, which requires us to take appropriate action against those individuals in breach.

If we conclude that a person has made false allegations maliciously, that person may be subject to disciplinary action – see the section on protections for whistleblowers, below.

If the whistleblowing disclosures are not proven, and there is no evidence of other inappropriate conduct, no further action will be taken.

Whatever the outcome, if the whistleblower can be contacted, the decision maker will advise them that the matter has been addressed, depending on confidentiality requirements by region. While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and in an appropriate way. By using this policy, you can help us to achieve this.

Depending on the nature and severity of the complaint or misconduct, UNiDAYS may implement a range of corrective actions, including but not limited to: strengthening internal controls, taking disciplinary action against those responsible, making necessary policy, training, structural or procedural changes and/or other steps to address the concern.

If you are not happy with the way in which your concern has been handled, you can raise it with one of the other internal key contacts, or externally as set out below.

External Disclosures:

The aim of this policy is to provide an internal mechanism for reporting, investigating, and remedying any wrongdoing in the workplace. In most cases, you should not find it necessary to alert anyone externally.

However, the law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. If you do not wish to disclose a whistleblowing matter to the contact people set out above, you may contact the Appropriate Regulatory Authority (*see Defined Terms*) for your region, as outlined below.

We encourage you to speak to an independent legal practitioner at any time if you would like legal advice or representation in relation to a whistleblowing disclosure. We also strongly encourage you to seek advice before reporting a concern to anyone external, such as the media, as those disclosures might not be protected. There also may be independent organisations that offer advice on whistleblowing matters available in your region. You can find the contact information for some of these organisations as well as contact details for EthicsPoint's confidential external Whistleblowing Hotline at the end of this policy.

Whistleblowing concerns usually relate to the conduct of our staff, but they may sometimes relate to the actions of a third party, such as a customer, supplier or service provider. Depending on your region, the law may allow you to raise a concern, the disclosure of which is in the public interest, with a third party, where you reasonably believe it relates mainly to their actions or something that is legally their responsibility. However, we encourage you to report such concerns internally first to the VP of People/Whistleblowing Officer, the Global General Counsel, the Chairman of the Board or through our confidential external telephone hotline and reporting system EthicsPoint.

Protection and Support for Whistleblowers and Others:

General Protections

UNiDAYS wants to ensure that whistleblowers who make disclosures in good faith or with a reasonable belief that the disclosure is in the public interest, depending on the region, do not suffer any detriment or disadvantage in retaliation or as a result, and that other staff members mentioned or involved in complaints and disclosures are also treated fairly. The protections set out below aim to achieve this. These protections may also be available to you if you make a disclosure to a legal practitioner to obtain legal advice or representation.

A complaint or whistleblowing disclosure made in good faith or with a reasonable belief that the disclosure is in the public interest, depending on the region, that turns out to be incorrect may also qualify for protection. However, protection is not available to a person who deliberately makes a false report.

Protection of identity and confidentiality

As noted above, you can make a whistleblowing disclosure anonymously, but doing so might make it more difficult for **UNiDAYS** or a relevant authority to assess and investigate your disclosure or provide you with relevant protections. It is your decision.

- If you have chosen to reveal your identity when making a whistleblowing disclosure, **UNiDAYS** may ask you to consent to us disclosing your identity and/or information that might lead to your identification, for example, if we consider that it would assist an investigation.
- If you choose not to give consent:
    - the person who knows your identity is permitted to disclose your identity only:
        - to an Appropriate Regulatory Authority;
        - to a legal practitioner to obtain advice;
        - in limited circumstances required by law, for example, where ordered by a court in legal proceedings; and/or
        - in accordance with applicable law.
    - **UNiDAYS** will take reasonable steps to make all relevant staff aware that:
        - they cannot disclose your identity, even to another **UNiDAYS** manager; and
        - they need to keep any notes, records or information about your whistleblowing disclosure secure; and
    - **UNiDAYS** may disclose any information (other than your identity) that aids its investigation, so long as it:
        - considers that the information in question aids its investigation but does not reveal your identity; and
        - takes steps it deems reasonable or helpful to reduce the risk that you will be identified as a result of disclosing that information.

The law states that whistleblowers must not suffer any detrimental treatment in response to raising a concern, the disclosure of which is in the

public interest. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the Whistleblowing Officer immediately. If the matter is not remedied, you should raise it formally using our Grievance Procedure. Staff must not threaten or retaliate against whistleblowers in any way. Anyone involved in such conduct will be subject to disciplinary action.

Protection of files and records

UNiDAYS maintains record-keeping and information sharing procedures with the aim of ensuring that all records are stored and handled securely.

All files and records created from an investigation should be retained under strict security, generally in a file accessible only by the person conducting the investigation– in compliance with the confidentiality requirements set by applicable law.

All complaints and documents relating to such complaints made through the procedures outlined in this policy shall be retained for at least six (6) years from the date of the complaint, after which time the information may be destroyed unless the information may be relevant to any pending or potential litigation, inquiry or investigation, in which case the information may not be destroyed and must be retained for the duration of that litigation, inquiry or investigation and thereafter as necessary.

No victimisation

'Victimisation' is what happens if a person is subjected to any detrimental treatment as a result of:

- making a complaint about a grievance and/or a whistleblowing disclosure; or
- someone else's belief that the person has made or will make a complaint or whistleblowing disclosure.

Victimisation can include, for example, bullying and harassment, termination of employment, physical violence or threats of physical violence, damage to reputation or unfavorable treatment such as:

- being excluded from activities or conversations at work;
- being demoted;
- being subject to disciplinary action;
- being denied a promotion or training opportunity;
- being given offensive nicknames or being the subject of offensive comments; or
- being excluded from pay increases.

Victimisation does not, however, include:

- administrative action that is reasonable to protect a whistleblower from detriment; or

- reasonable management action, such as setting high-performance standards, constructive feedback and legitimate advice and/or peer review.

Victimisation is strictly prohibited. You should immediately inform the VP of People/Whistleblowing Officer, Global General Counsel or the Chairman of the Board if you are subjected to victimisation, or any threat of victimisation so that **UNiDAYS** can take action.

The investigating officer may need to work with others to manage the risk of victimisation, including relevant managers, the People Team, or the Legal Team. The VP of People/Whistleblowing Officer, Global General Counsel or Chairman of the Board is expected to act in a timely manner to:

- protect you in the interim, which might include temporarily relocating you or the victimiser, or changing your reporting line;
- conduct a preliminary assessment of any alleged victimisation;
- if necessary and if you consent, refer the matter to senior management for further investigation; and
- if the allegation of victimisation is substantiated, and if you consent, refer the matter to a decision maker for further action.

Other staff members mentioned or involved in complaints and disclosures also need to be treated fairly. This is partly achieved by their involvement being kept reasonably confidential in accordance with the protections set out above. It also means that no decisions should be made that cause them detriment without proper investigation.

If you raise a concern about someone victimising you and that person is not an employee, **UNiDAYS** will assess, on a case-by-case basis, the appropriate steps for it to take.

Other whistleblower protections

Depending on the region, whistleblowers who make disclosures in good faith may have additional protections under legislation, including:

- whistleblowers are not subject to any civil, criminal or administrative liability (including disciplinary action) for making the disclosure;
- no contractual or other remedy can be enforced, and no contractual or other right can be exercised against a whistleblower on the basis of the disclosure;
- if the disclosure is made to an Appropriate Regulatory Authority, or is a public interest/emergency disclosure, then the information may not be admissible in criminal proceedings or for the imposition of a penalty against a whistleblower; and
- whistleblowers may also have the right to seek compensation through the courts if they suffer loss, damage or injury because of a disclosure. Other remedies may be available depending on the type of detriment suffered. For example, a court may grant an injunction to stop victimisation, require an apology to be given, or to reinstate a whistleblower who has been victimised by termination of employment.

Involvement in Wrongdoing:

UNiDAYS may discipline anyone found to have breached this policy, for example:

- unlawfully discriminated against, harassed, vilified or bullied another, or otherwise acted inappropriately;
- victimised a complainant or whistleblower;
- disclosed information in breach of our confidentiality rules; or
- lied about a complaint or made a complaint maliciously, or otherwise in bad faith.

Disciplinary action can involve termination of employment or contractor arrangements without notice on the grounds of gross misconduct.

Some of the protections under this policy might also not be available to you if you are found to have been involved in wrongdoing that is the subject of a complaint or whistleblowing disclosure.

German Whistleblower Protection Act:

The following applies to those whistleblowers located in Germany and/or affiliated with **UNiDAYS** GmbH: This policy shall apply in addition to the German Whistleblower Protection Act (the "Act"), which shall supersede this policy if the provisions of the Act and those of this policy contradict. Such differences include but are not limited to:

- The accessibility under this policy including, in relation to **UNiDAYS**, employees, former employees, and prospective employees, employees of the company's suppliers, job applicants, persons similar to employees (that is, persons, who while being self-employed entrepreneurs, are economically dependent on a client and, similar to employees, are in need of social protection), self-employed persons, members of executive bodies (for example, management, executive board, or supervisory board), natural persons who support the whistleblower, persons who are the subject of a report or disclosure, and other persons affected by a report or disclosure.
- A deadline of seven days for the internal reporting channel to confirm receipt of the report of a whistleblower disclosure and three months from that confirmation for the internal reporting office to provide feedback to the maker of the report regarding planned and taken follow-up measures, if the investigations or rights of others are not affected.
- The requirement for reports to be documented in a permanently retrievable manner and a deletion period of three years after termination of the proceedings.
- Protection from any retaliation or detrimental treatment is provided in accordance with the Whistleblower Protection Act and is subject to, among other things, the condition that the whistleblower or any person assisting the whistleblower at the time of the report or disclosure had reasonable grounds to believe that the information reported or disclosed was true and related to violations within the scope of the Whistleblower Protection Act or had reasonable grounds to believe that the scope of the Whistleblower Protection Act would apply at the

time of the report or disclosure.

Defined Terms by Region

UK:

1. Protected Disclosure: Whistleblowing is protected only if it constitutes a 'protected disclosure' (s 43B of ERA 1996).
   In order for a disclosure to be considered as a protected disclosure three requirements need to be satisfied:
   - there needs to be a disclosure;
   - the disclosure must be a 'qualifying disclosure' (as defined by section 43B); and
   - it must be made by the worker in a manner consistent with that set out at section 43C to 43H of ERA 1996.
2. Appropriate Regulatory Authority: A list of prescribed people and bodies can be found here to identify the Appropriate Regulatory Authority which handles the subject matter of your whistleblowing concern.

AUS:

1. Protected Disclosure: Whistleblowing is protected only if it constitutes a 'protected disclosure'
2. Appropriate Regulatory Authority: You can contact the Australian Securities and Investment Commission (ASIC) or the Australian Prudential Regulation Authority (APRA) to make a whistleblowing disclosure under the Corporations Act, and you should refer to their policy about how the disclosure might be handled. You can also make a protected disclosure under the Tax Act to the Australian Commissioner of Taxation, in which case you should refer to their policy about how disclosures might be handled.
3. Permitted External Official: You may make a protected disclosure to an auditor or actuary.

US:

1. Appropriate Regulatory Authority: In New York, an employee may direct a whistleblowing complaint to the New York Commissioner of Labor. An employee may also disclose an illegal activity, policy, or practice of the employer that presents a substantial and specific danger to the public health or safety to a public body such as a legislative body, a judicial officer, an administrative agency, or law enforcement agency only after the employee has brought the violation to the attention of their supervisor and then given the employer a reasonable opportunity to correct the activity, policy, or practice. Federally, employees may also make whistleblowing disclosures to OSHA, the SEC, or the EEOC but each agency has different rules on maintaining the anonymity of a disclosure and we advise you to seek legal counsel if you are concerned prior to any disclosure.

DE:

1. Protected Disclosure: Whistleblowing is protected only if it constitutes a 'protected disclosure' in accordance with the German

Whistleblower Protection Act. In this respect, whistleblowers can and should provide information about, i.a.,

- violations that are punishable by law;
- violations that are subject to fines, insofar as the violated provision serves to protect life, limb or health or to protect the rights of employees or their representative bodies;
- as well as other violations of federal and federal state legislation and directly applicable legal acts of the European Union and the European Atomic Energy Community, which are listed in detail in the Act;

2. Appropriate Regulatory Authority: Additional specialised reporting channels have been established by the Federal Office of Justice (Bundesamt für Justiz), the German Federal Cartel Office (Bundeskartellamt), or the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht). Additional reporting channels at the state level are also available.

Contacts:

- Chief Operating Officer: tamara.castelli@myunidays.com (to stand in for VP of People/Whistleblowing Officer or Global General Counsel as needed)
- VP of People/Whistleblowing Officer: See Chief Operating Officer
- Global General Counsel: bita.goldman@myunidays.com
- Chairman of the Board: matt.atkinson@myunidays.com
- **Confidential External Whistleblowing Hotline**:

  EthicsPoint provided by Navex:

  UK: 0808-234-7287

  AUS: 1-800-139957

  USA: 1-855-229-9304

  DE: 0800-1800042

  IN: direct access number for India: **000-117** at the English prompt dial **855-229-9304**

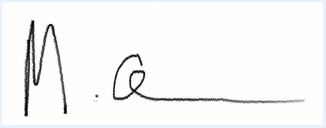
  Website:http://makingmyunidaysbetter.ethicspoint.com/

- Protect (in the UK): Helpline: 0203 117 2520
- OSHA (in the US): 800-321-OSHA (6742)
- SEC (in the US): (202) 551-4790
- EEOC (in the US)
- Australian Human Rights Commission (for discrimination claims)
- Safe Work Australia (for Workplace Health and Safety Claims in NSW)
- Fair Work Commission (Australia) (For disputes arising under enterprise agreements, other registered agreements or awards)
- Federal Office of Justice (Bundesamt für Justiz) (DE)
- German Federal Cartel Office (Bundeskartellamt) (DE)
- Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht) (DE)

Policy Administration

Policy Owner:	Legal
Scope:	Global
Effective date:	03 April 2025
Policy Number:	LP-0001

Policy Approvals

Date	Department	Approver	Signature
11/10/2024	Legal	Bita Goldman	
19/12/2024	EXEC / People	Jon Hawley	
19/12/2024	Chairman of the Board	Matt Atkinson	

Change History

Date	Version	Summary of Changes	Author
02-September-2021	1.0	Policy creation	Edward Reilly

19-December-2024	2.0	Policy revision	Jessica Greenberg

Whistleblowing Privacy Notice

This Whistleblowing Privacy Notice describes how MYUNIDAYS LTD and its affiliates (UNiDAYS Inc., UNiDAYS GmbH, UNiDAYS Australia Pty Limited and UNiDAYS Private Limited, collectively "UNiDAYS", "we" or "our") collect and process personal information about an individual ("you" or "your") as part of a whistleblowing disclosure made in connection with UNiDAYS' Whistleblowing Policy and any follow up investigation into a disclosure.

UNiDAYS is a data controller of your personal information. UNiDAYS has appointed a Data Protection Officer (DPO). If you have any questions about this privacy notice or our data protection practices please contact our Data Protection Officer using the contact details under the 'How to contact us' section of this notice.

If you are an employee of UNiDAYS, this Whistleblowing Privacy Notice supplements UNiDAYS' Employee Privacy Notice, which applies to UNiDAYS' collection of personal information outside of the whistleblowing context.

If you are a resident of the United States, please see the additional Notice for Citizens of the United States at the end of this Privacy Notice.

What personal information do we collect?

When a whistleblowing disclosure is made or when we carry out a follow up investigation into a disclosure, we may collect and process any of the following categories of personal information about you:

- Name
- Location where the incident occurred (including address)
- City
- State / Province
- Zip / Postal Code
- Country
- Confirmation on whether you are a UNiDAYS employee or not
- Full Name
- Phone Number
- Email address
- Age
- Gender
- Details of the best time to contact you
- Identity(ies) of the person(s) engaged in the behavior being disclosed (including name and title)
- Details of the matter being disclosed (e.g. the nature of the matter, date and time when the incident or violation occurred, how you became aware of the violation, how long the problem has been going on, identity of individuals who attempted to conceal the problem, documents that you upload to

support the disclosure and any other details regarding the alleged violation including the locations of witnesses and any other information that could be valuable in the evaluation and ultimate resolution of the situation)
- Evaluation of internal UNiDAYS communications such as business email correspondence or instant messaging records
- Evaluation of internal business documents
- Personal information relating to criminal convictions and offences - we may also collect personal information about you which may allow conclusions to be drawn about crimes or criminal convictions affecting you e.g. if this personal information is disclosed to us as part of a disclosure or is discovered during a follow up investigation. However, we will only process this personal information in accordance with the relevant provisions of applicable data protection law
- Sensitive personal information - we may also collect sensitive personal information about you if this personal information is disclosed to us as part of a disclosure or is discovered during a follow up investigation. This may include, for example, data revealing racial or ethnic origin, genetic data, data concerning an individual's sex life or sexual orientation, health data, biometric data or data on political or religious beliefs. However, we will only process this personal information in accordance with the relevant provisions of applicable data protection law

How do we collect your personal information?

UNiDAYS collects your personal information in the following ways:

- Directly from you - when you make a whistleblowing disclosure or as part of a follow up investigation
- Indirectly from you - when a whistleblowing disclosure has been made and you are named in the disclosure or as part of a follow up investigation

How will we use your personal information?

UNiDAYS collects and processes your personal information for the following purposes:

- Receiving and handling whistleblowing disclosures
- Cooperating with any external party (e.g. regulator) to the extent you make a protected disclosure to a third party
- Carrying out an investigation upon receiving a whistleblowing disclosure
- Protecting the privacy, rights and safety of the individual making the disclosure, witnesses and third parties mentioned in the disclosure as well as the individual(s) named in the disclosure
- Preventing future misconduct
- Communicating with you to provide updates on the status of the investigation

How do we share your personal information?

We will only disclose your personal information to third parties where required by law or to parties who require the information to assist us with administering our Whistleblowing Policy or investigating potential misconduct, for example, our authorised employees, contractors, or designated agents, our affiliate companies, regulators, law enforcement, or third-party service providers. Third-party service providers may include, but are not limited to, Navex (the

third-party provider that operates our Whistleblowing Reporting Portal and the External Whistleblowing Hotline), outside counsel, consultants, auditors, and investigators. Third-party recipients, including third-party service providers, may be located outside of your home country.

We contractually require all our third-party service providers to implement appropriate security measures to protect your personal information consistent with our policies and any data security obligations applicable to us. We do not permit our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specific purposes in accordance with our instructions.

We may also disclose your personal information for the following additional purposes where permitted or required by applicable law:

- To our affiliates (based in the United States, Germany, Australia and India) for the purposes set out in this Whistleblowing Privacy Notice and as necessary to perform our employment contract with you
- To comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders. When we disclose your personal information to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal information necessary for the specific purpose and circumstances
- To protect the rights and property of UNiDAYS
- During emergency situations or where necessary to protect the safety of persons
- For additional purposes with your consent, where the law requires such consent.

What is our lawful basis for processing your personal information?

We rely on the following lawful bases under applicable data protection law to process your personal information:

- Performance of a contract - if you are a UNiDAYS employee, we may process your personal information when carrying out an investigation following a disclosure, this processing is necessary as part of the employment contract between you and UNiDAYS
- Compliance with a legal obligation to which we are subject - for example if a whistleblowing system is required by applicable law, this means we process your personal information in so far as it is necessary for the fulfillment of our legal obligations
- Legitimate Interest - we may process your personal information in order to protect UNiDAYS' or a third party's legitimate interests. These legitimate interests may include the following but are not limited to

    - In order for UNiDAYS to establish, exercise or defend itself against legal claims
    - To continuously improve UNiDAYS' internal compliance reporting structures
    - In order for UNiDAYS to support individuals who are the subject of a disclosure - the processing associated with carrying out the follow up investigation is necessary to determine whether the accusations against a named individual are valid or not. This processing is therefore a legitimate interest of a third party.

To the extent we collect any sensitive personal personal information that you provide as part of a disclosure or that we discover as part of a follow investigation, we will process this personal information for the purpose of administering our Whistleblowing Policy and investigating potential misconduct when the processing is necessary:

- For carrying out our legal obligations and protecting our rights under applicable laws
- To protect the vital interests of an individual

- To establish, exercise, or defend legal claims
- For reasons of substantial public interest

How do we store your personal information?

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal information for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of administering our Whistleblowing Policy and investigating potential misconduct.

To determine the appropriate retention period for personal information, we consider our legal retention obligations, the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes we process your personal information for, and whether we can achieve those purposes through other means.

Local laws permit UNiDAYS to retain records of whistleblower allegations and complaints for certain purposes, such as:

- Preserving potential evidence if the matter results in a criminal, civil, or regulatory action; and
- To establish, exercise, or defend legal claims.

Under some circumstances, we may anonymize your personal information so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent.

How do we protect your personal information?

UNiDAYS takes care to secure and safeguard your personal information using various technological measures as required by applicable law. Like any other organisation, UNiDAYS cannot fully eliminate security risks associated with the processing of personal information but UNiDAYS uses technical, physical, and administrative safeguards intended to protect the personal information that we process. Our safeguards are designed to provide a level of security appropriate to the risk of processing your personal information and include (as applicable) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and a procedure for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal information.

Where do we process your personal information?

Generally, we process personal information in the United Kingdom, Ireland and the United States, depending on the circumstances. We transfer personal information only as permitted by applicable law.

Your personal information may be transferred to and processed someplace other than where you live. These other jurisdictions may have privacy laws that are different from the laws of where you reside (and, in some cases, not as protective).

The third parties with whom or which we share personal information, as described under the 'How do we share your personal information' section of this notice, are located in and transfer personal information to various jurisdictions around the world.

Where your personal information is transferred by us or on our behalf, we use appropriate safeguards to protect your personal information in accordance with this notice and applicable law. These safeguards include entering into Standard Contractual Clauses for transfers of personal information where applicable. We

also may require additional safeguards depending on where personal information is transferred. Please contact us using the contact details provided under the 'How to contact us' section of this notice for more information.

When we share personal information with a third party acting as our processor e.g. Navex that operates our Whistleblowing Reporting Portal and the External Whistleblowing Hotline, we do so subject to contractual obligations that require that the processor protect your personal information in accordance with this notice.

What are your data protection rights?

Under applicable data protection law, you have rights including:

- **The right to access** – You have the right to ask us for copies of your personal information.
- **The right to rectification** – You have the right to request that UNiDAYS correct any information you believe is inaccurate. You also have the right to request UNiDAYS to complete the information you believe is incomplete.
- **The right to erasure** – You have the right to request that UNiDAYS erase your personal information, under certain conditions.
- **The right to restrict processing** – You have the right to request that UNiDAYS restrict the processing of your personal information, under certain conditions.
- **The right to data portability** – You have the right to request that UNiDAYS transfer the personal information that we have collected to another organization, or directly to you, under certain conditions.
- **Your right to object to processing** - You have the right to object to the processing of your personal information in certain circumstances.

If you are a resident of the United States, please see the additional Notice for Citizens of the United States at the end of this Privacy Notice which contains information on the additional data subject rights that apply to you.

If you would like to exercise any of the above rights, please contact us using the contact details under the 'How to contact us' section of this privacy notice. We will review your request as soon as reasonably practicable and respond within the time periods required by applicable law. In any request you submit to us, please make clear the personal information that is the subject of your request.

We respond to all requests we receive from individuals wishing to exercise their privacy rights in accordance with applicable data protection laws. Please know that the rights described above are not automatic rights and may not apply in all circumstances. When this occurs, we will notify you in our response to you.

The above rights are not absolute and applicable law may allow or require us to deny your request, or we may have destroyed, erased, or made your personal information anonymous in accordance with our record retention obligations and practices. If we cannot respond to your request, we will inform you of the reasons why, subject to any legal or regulatory restrictions. For example, we may deny requests to protect the confidentiality and integrity of an investigation.

Changes to this privacy notice

UNiDAYS keeps this privacy notice under regular review. This privacy notice was last updated on 11 October 2024.

If we would like to use your previously collected personal information for different purposes than those we notified you about at the time of collection, we will provide you with notice and, where required by law, seek your consent, before using your personal information for a new or unrelated purpose. We may process your personal information without your knowledge or consent where permitted or required by applicable law or regulation.

How to Contact Us

If you have any questions about this privacy notice, the personal information we hold on you, or you would like to exercise any of your data protection rights, please do not hesitate to contact us.

- Email us at: DPO@myunidays.com; or
- Write to us at: 25 Epworth Street, City Road, London, EC1Y 1AA, United Kingdom.

Alternatively, you may contact our Our European representative:

- By email: unidays_eu_representative@planit.legal; or
- By post: PLANIT//LEGAL, Jungfernstieg 1 20095, Hamburg, Germany

How to complain

Should you wish to report a complaint or if you feel that UNiDAYS has not addressed your concern in a satisfactory manner, you may contact the Information Commissioner's Office at the following address or website: Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Helpline number: 0303 123 1113, ICO website: https://www.ico.org.uk.

If you are in an EU member state, you may contact your local data protection supervisory authority using the contact details here.

If you are in a country outside the UK/EEA and wish to make a complaint to the relevant data protection authority, please contact us and we will provide you with details of how to contact the data protection authority in the country where you are based.

NOTICE FOR CITIZENS OF THE UNITED STATES - WHISTLEBLOWING

Last Updated: October 2024

Your privacy is our priority. We appreciate that you entrust us with your personal information and want you to know that we respect your privacy. Therefore, UNiDAYS has taken one approach to respecting and protecting US citizens' privacy rights. In other words, we combined the highest degree of privacy rights granted by various US state laws so that the highest degree of privacy rights can be exercised by a US citizen. For completeness, we have also added details of some state laws for awareness.

What rights can I exercise?

- **Right to Know/Access**: You have a right to request that we disclose, up to two times per year: (1) the categories of personal information we have collected, sold, or shared about you; (2) the categories of sources from which your personal information was collected, sold, or shared; (3) the business or commercial purpose for collecting, selling, or sharing your personal information; (4) the categories of third parties to whom we've sold, shared, or disclosed for a business purpose your personal information; and (5) the specific pieces of personal information we have collected about you. You have a right to access your personal information subject to certain exceptions, and obtain a copy of the personal information in a portable format.
- **Right to Delete**. You have a right to request that we delete the personal information we hold about you, subject to certain exceptions available under applicable law.
- **Right to Correct**. You have a right to ask that we correct inaccurate or incorrect personal information we have collected about you, subject to certain exceptions available under applicable law. Also you can login to your account and make any correction to your personal information, as may be necessary.
- **Right to Opt-Out.** You have a right to opt-out of the sale or sharing of your personal information or the use of your personal information for targeted advertising. Please note that UNiDAYS does not sell or share any personal information collected in connection with a whistleblowing disclosure / follow up investigation, nor use your personal information for targeted advertising purposes.
- **Right to Non-Discrimination**. You have a right to exercise the above rights without being discriminated against.

How do I exercise my rights?

You can exercise your rights at any time as follows:

- To submit a request for Right to Delete, please contact us at dpo@myunidays.com;
- To submit a request for Right to Know/Access, please contact us at dpo@myunidays.com;
- To submit a request for Right to Correct, please contact us at dpo@myunidays.com.

Notice For California Residents - California Consumer Privacy Act

Definitions

- **Personal information**. Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to you or your household.
- **Sensitive personal information**. Social security number, driver's license number, state identification card, passport number, account log-in and password, financial account and password, debit or credit card number and access code, precise geolocation information, race, ethnic origin, religious or philosophical beliefs, union membership, the content of your mail, email or texts other than those communications with us, genetic data, biometric information, health information, and information that concerns your sex life or sexual orientation.
- **Sell, sale, or sold**. Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or other means, your personal information to a third party for money or other valuable consideration.
- **Share, shared, or sharing**. Shearing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or other means, your personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

Your Rights

You may designate an authorized agent to submit a request for any of the rights below on your behalf. When you use an authorized agent, you must provide the authorized agent with a signed written permission to do so. We may also ask you to verify your own identity directly with us. **The process for exercising the below rights is set out above under the heading 'How do I exercise my rights' here**.

- **Right to Know**: You have a right to request that we disclose, up to two times per year: (1) the categories of personal information we have collected, sold, or shared about you; (2) the categories of sources from which your personal information was collected, sold, or shared; (3) the business or commercial purpose for collecting, selling, or sharing your personal information; (4) the categories of third parties to whom we've sold, shared, or disclosed for a business purpose your personal information; and (5) the specific pieces of personal information we have collected about you.
- **Right to Delete**. You have a right to request that we delete the personal information we hold about you, subject to certain exceptions available under applicable law.
- **Right to Correct**. You have a right to ask that we correct inaccurate or incorrect personal information we have collected about you, subject to certain exceptions available under applicable law. Also you can login to your account and make any correction to your personal information, as may be necessary.
- **Right to Opt-Out of the Sale or Sharing of Your Personal Information**. You have a right to opt-out of the sale or sharing of your personal information. Please note that UNiDAYS does not sell or share any personal information collected in connection with a whistleblowing disclosure / follow up investigation.
- **Right to Non-Discrimination**. You have a right to exercise the above rights without being discriminated against.

Notice of Collection

Below we identify the categories of personal information we may collect about California residents (and may have collected in the 12 months preceding the date this Notice for Citizens of the United States was last updated). This list includes information about: (1) whether this information includes sensitive personal information; (2) the categories of sources from which the personal information was collected; (3) the business or commercial purpose for collecting, selling, or sharing the personal information; and (4) the categories of third parties with whom we disclose such information.

- **Identifiers**: Information such as your name, country of residence, location where the incident occurred (including address), zip/postal code, state/province, city, email address, phone number, confirmation on whether you are a UNiDAYS employee, details of the best time to contact to you, identity(ies) of the person(s) engaged in the behaviour being disclosed (including name and title), details of the incident being disclosed (e.g. the nature of the matter, date and time when the incident or violation occurred, how you became aware of the violation, how long the problem has been

going on, identity of individuals who attempted to conceal the problem, documents that you upload to support the disclosure and any other details regarding the alleged violation (including the locations of witnesses and any other information that could be valuable in the evaluation and ultimate resolution of the situation).

- **Sensitive personal information and characteristics of protected classifications under California law:** we may also collect sensitive personal information about you if this personal information is disclosed to us as part of a disclosure or is discovered during a follow up investigation. This may include, for example, age, gender, data revealing racial or ethnic origin, genetic data, data concerning an individual's sex life or sexual orientation, health data, biometric data or data on political or religious beliefs. However, we will only process this personal information in accordance with the relevant provisions of applicable data protection law. We may also collect personal information about you which may allow conclusions to be drawn about crimes or criminal convictions affecting you e.g. if this personal information is disclosed to us as part of a disclosure or is discovered during a follow up investigation. However, we will only process this personal information in accordance with the relevant provisions of applicable data protection law.
- **Audio and Visual Information:** audio, electronic, visual information that you provide as part of a disclosure or that is discovered as part of a follow up investigation.
- **Internet or other Electronic Network Activity Information**: evaluation of internal UNiDAYS communications such as business email correspondence or instant messaging records.
- **Commercial Information**, Not Applicable
- **Geolocation Information**, Not Applicable
- **Inferences**, Not Applicable

<table>
<tr><th>Disclosure</th><th>Categories</th><th>Description</th></tr>
<tr><td rowspan="7">How do we collect this information?</td><td>Identifiers</td><td rowspan="3">We collect these categories of information from you: 1. directly when you make a whistleblowing disclosure or as part of a follow up investigation; and 2. indirectly from you - when a whistleblowing disclosure has been made and you are named in the disclosure or as part of a follow up investigation.</td></tr>
<tr><td>Sensitive Personal Information</td></tr>
<tr><td>Characteristics of protected classifications under California law</td></tr>
<tr><td>Audio and Visual Information</td><td rowspan="2">We collect this category of information from you: 1. directly when you make a whistleblowing disclosure or as part of a follow up investigation; and 2. indirectly from you - when a whistleblowing disclosure has been made and you are named in the disclosure or as part of a follow up investigation.</td></tr>
<tr><td>Internet or other electronic activity information</td></tr>
<tr><td>Commercial information</td><td>Not Applicable</td></tr>
<tr><td>Geolocation information</td><td>Not Applicable</td></tr>
<tr><td>Inferences</td><td>Not Applicable</td></tr>
<tr><td>Does this include sensitive personal information?</td><td colspan="2">Yes, to the extent that sensitive information is provided as part of a disclosure or is discovered as part of a follow up investigation.</td></tr>
<tr><td>Is the information "sold" or "shared"?</td><td colspan="2">No.</td></tr>
</table>

What is our business purpose for collecting your information?	For a list of the purposes for which UNiDAYS collects your personal information, please click here.
Who do we disclose this information to?	For a list of the categories of third parties with whom we may have disclosed the information, please click here.
How long do we keep this information?	For details of how we store your personal information, please click here.

Notice of Disclosure for a Business Purpose

In the last 12 months preceding the date this Privacy Notice was last updated, we have shared with third parties, for a business or commercial purpose, the types of personal information described in the "Notice of Collection" section above. For a list of the categories of third parties with whom we may have disclosed the information, please click here.

Notice of Sale and Sharing

UNiDAYS does not sell or share any personal information collected in connection with a whistleblowing disclosure or as part of any whistleblowing investigation.

Notice of Processing Sensitive Personal Information

We do not use California residents' sensitive personal information to infer characteristics about California residents.

US-wide Metrics on Consumer Rights Requests for 2022

The following chart shows details about the consumer rights requests we received in the United States from January 1, 2022 to December 31, 2022 in relation to whistleblowing disclosures and investigations:

Request Type	Received	Complied with in whole	Complied with in part	Denied	Average Days to Respond
Requests to Know	0	NA	NA	NA	NA
Requests to Delete	0	NA	NA	NA	NA

Requests to Opt-Out of Sale	NA	NA	NA	NA	NA

California's "Shine in the Light" law

If you are a California resident, you have the right to request information from us once per calendar year regarding the customer information we share with third parties for the third parties' direct marketing purposes. Please note that in relation to any personal information collected in connection with a whistleblowing disclosure, UNiDAYS does not share this personal information with third parties for the third parties' direct marketing purposes.

Notice For Virginia, Colorado, Utah, and Connecticut Residents

Definitions

- **Personal information**. Information that is linked or reasonably linkable to an identified or identifiable individual.
- **Sensitive personal information**. Information that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, the processing of genetic or biometric data for the purpose of uniquely identifying an individual, personal information collected from a known child, or precise geolocation data.
- **Sell, sale, or sold**. The exchange of personal information for monetary or other valuable consideration.
- **Targeted advertising**. Displaying advertisements to a consumer where the advertisement is selected based on personal information obtained or inferred from that individual's activities over time and across nonaffiliated Internet web sites or online applications to predict such individual's preferences.

Notice of Collection

To learn more about the categories of personal information we collect about you and how we use it, please click here. To learn more about the categories of third parties with whom we may share your personal information, please click here. **The process for exercising the below rights is set out above under the heading 'How do I exercise my rights' here**.

Your Rights

- **Right to Know and Access**: You have a right to know whether UNiDAYS is processing your personal information, access such personal information subject to certain exceptions, and obtain a copy of the personal information in a portable format.
- **Right to Delete**. You have a right to request that we delete your personal information.
- **Right to Correct**. You have a right to ask that UNiDAYS correct the personal information it has about you, subject to certain exceptions.
- **Right to Opt-Out**. You have a right to opt-out of the sale or use of your personal information for targeted advertising. Please note that UNiDAYS does not sell any personal information collected in connection with a whistleblowing disclosure / follow up investigation, nor use this personal information for targeted advertising purposes.
- **Right to Non-Discrimination**. You have a right not to be discriminated against for the exercise of your rights described herein.

Notice for Nevada Residents

If you are a Nevada resident, you have the right to submit a request directing us not to make any sale of your personal information. In connection with a whistleblowing disclosure or as part of any whistleblowing investigation, UNiDAYS does not sell your personal information under Nevada law. However, to

request email confirmation that we do not sell your personal information, please send an email to dpo@myunidays.com with "Request for Nevada Privacy Information" in the subject line and in the body of your message. We will provide the requested information to you via an email response.