Nestle European Pension Fund (NEPF) - Institution for Occupational Retirement Provision
FSMA identification number 50.111
Rue de Birmingham 221 - 1070 Brussels

NEPF data privacy policy

In the context of the harmonization of the data privacy laws across Europe, the European Union has adopted the General Data Protection Regulation[1] (hereafter the "GDPR"). Within the framework of the GDPR, Nestlé European Pension Fund (hereafter "NEPF") and the Sponsoring Undertakings have to comply with a certain set of requirements and obligations.

NEPF has laid down the main principles it follows in relation to data privacy in the context of the occupational pension plans of which the management and administration are entrusted to NEPF (hereafter "the Pension Plans") in the present data privacy policy In this policy, all the details such as the obligations of the controllers, the process by which a personal data breach has to be reported, the data subjects' rights and the security measures put in place are explained.

1) General information

a) Definitions

Authorised Users means persons who, in the performance of their role within NEPF or the Sponsoring Undertakings, are authorised to process Personal Data under the instructions of NEPF and/or the Sponsoring Undertakings in the context of management and implementation of the Pension Schemes. It concerns amongst others: staff members of the Sponsoring Undertakings, directors of NEPF, members of the Management Committee of NEPF, members of the Investment Committee of NEPF, members of the Audit & Compliance Committee of NEPF, members of the Pension Councils, members of any other operational body or advisory committee set up by NEPF.

Beneficiary means the persons who are possibly entitled to a death benefit in accordance with the death cover as provided in the applicable Pension Plans. In this framework a distinction is made between the potential beneficiaries and the effective beneficiaries.

Potential Beneficiaries are the persons mentioned in the beneficiary order as determined in the Pension Plans, who are possibly entitled to a death benefit in case of decease of the Plan Member (for instance the partner, the children, the Beneficiaries as designated by means of a beneficiary form, if any) and who are indirectly registered by NEPF and/or the Sponsoring Undertakings in the context of the registration of the Plan Member.

Effective Beneficiaries are the persons who are effectively entitled to a death benefit after decease of the Plan Member in accordance with the beneficiary order and the conditions as determined in the Pension Plan rules.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of naturals persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Breach means a 'personal data breach' as defined in the GDPR, i.e. 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

Controller is the entity that determines the purposes, conditions and means of the processing of personal data. In the context of the management and implementation of the Pension Plans, NEPF and the Sponsoring Undertakings are Joint Controllers.

Data Subject is the person to whom belongs the personal data that are processed and that allows anyone to identify her/him. In the context of the management and implementation of the Pension Plans, Data Subjects are the Plan Members and their Beneficiaries.

European Economic Area ("**EEA**") currently includes the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK.

Personal Data means any information relating to an identified or identifiable natural person. In the context of the management and implementation of the Pension Plans, it concerns the Personal Data of the Plan Members and their Beneficiaries.

Processing is defined in the GDPR as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

Processor is an entity, which processes personal data on behalf of the Controller. In the context of NEPF, Processors are mainly the pension plan administrators or the accounting firms.

Plan Member means the (former) employee of the Sponsoring Undertakings who is affiliated to one or more Pension Plans, in accordance with the affiliation conditions as determined in the applicable pension plan rules.

Sensitive personal data means Personal Data revealing a person's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- data concerning health or sex;
- data relating to criminal convictions and offences or related security measures;

Sponsoring Undertakings means the companies who entrusted the management and administration of the Pension Plans to NEPF. At the time of adopting this Policy the Sponsoring Undertakings are, in Belgium: Nestlé Belgilux NV, Coordination Center Nestlé NV, Nestlé Catering Services NV, Nespresso Belgique NV, Lactalis Nestlé Produits Frais NV, Galderma Benelux NV; in Luxembourg: Nestlé Treasury Center Europe SA, Nestlé Finance International Ltd,

Nestlé Treasury International SA, Nespresso Luxembourg SA, Nestlé Catering Services SA; in Ireland: Nestlé (Ireland) Ltd, Galderma (UK) Ltd, Nespresso UK Ltd, Wyeth Nutritionals Ireland Ltd.

b) Purposes of the Processing

The purpose of the Processing activities of the Controllers is to manage and administer the Pension Plans. To achieve this purpose, the Controllers have to process a certain number of Personal Data, in order to be able to:

- calculate the pension, death and/or disability benefits of the (former) Plan Members and/or their Beneficiaries.
- administer the Pension plan (including the administration of the affiliation and the departure of Plan Members);
- draft and communicate the annual benefit statements, as well as other (historical) overviews and calculations;
- calculate the contributions to finance the Pension Plans;
- draft and communicate information to the Plan Members and the Beneficiaries (departure forms, liquidation forms , etc.);
- execute individual and collective transfers;
- do the financial management and accounting of NEPF;
- report to the FSMA, NBB, tax administration and to other authorities where appropriate; including communication or correspondence with these authorities;
- report to the Federal Pensions Service (Pension Registry) and communication or correspondence with the Federal Pensions Service;
- carry out the Sigedis declarations (DB2P);
- dispose information on an online tool ;
- ...

c) Main principles for the Processing

NEPF and the Sponsoring Undertakings respect the privacy of the Plan Members and the Beneficiaries whose Personal Data are processed in the context of the management and administration of the Pension Plans, and are committed to protect their Personal Data in accordance with the GDPR and the Legislation and Regulations concerning Data Protection.

Furthermore, NEPF and the Sponsoring Undertakings comply with the following principles when Processing the Personal Data in the context of the management and administration of the Pension Plans :

- **Lawful data processing** - NEPF and the Sponsoring Undertakings process Personal Data lawfully in order to (i) comply with their legal obligations in accordance with the Act of 28 April 2003 concerning occupational pensions and/or the Act of 27 October 2006 concerning the supervision of institutions for occupational retirement provision and their respective implementing decrees, and to (ii) implement the Pension Plans.

- **Purposes and purpose limitation** - NEPF and the Sponsoring Undertakings collect and process Personal Data for the following legitimate purposes: the management and administration of the Pension Plans.
- **Data minimisation** - NEPF and the Sponsoring Undertakings limit the Processing of Personal Data to what is necessary in the context of the management and implementation of the Pension Plans.
- **Accuracy of Personal Data** - NEPF and the Sponsoring Undertakings take every reasonable measure to ensure that the Personal Data are accurate and that they are rectified or erased without delay when they would no longer be accurate.
- **Limitation of Processing and storage** - NEPF and the Sponsoring Undertakings shall not process and store the Personal Data any longer than necessary for the abovementioned purposes.
- **Security measures** - NEPF and the Sponsoring Undertakings will implement appropriate technical and/or organisational measures for the security of the Personal Data of the Scheme Members and the Beneficiaries, in order to avoid Breaches. These measures shall be regularly reviewed and updated if necessary. In case of a Breach, the IORP and the Sponsoring Undertakings shall take appropriate measures to establish its scope and consequences, to eliminate the Breach as quickly as possible and, if applicable, to limit its impact for the concerned Plan Members and/or Beneficiaries.

d) Personal Data under Processing

NEPF will limit the Processing of Personal Data and Sensitive Personal Data to the data that are reasonably appropriate and relevant to the purpose, and will process the Personal Data only as long as necessary for the above-mentioned purpose. NEPF will take all reasonable steps to remove any data that is not required for the above-mentioned purpose.

NEPF and the Sponsoring Undertakings will take all reasonable measures to keep accurate, complete and up-to-date the Personal Data of the Plan Members and Beneficiaries. If there are inaccuracies regarding the Personal Data, the Plan Member or Beneficiary needs to inform the human resources department, by following the HR processes in place. The Sponsoring Undertaking will then immediately inform NEPF about the inaccuracy, so that the necessary corrections can be made. . For the Beneficiary, they can inform the local pension plan administrator about any inaccuracies.

The below Personal Data categories, are or may be processed by NEPF and/or the Sponsoring Undertakings. Those categories refer to different types of Data Subjects:

- Plan Members,
- Beneficiaries of the Plan Members (such as partner, children, etc.)

Categories of Personal Data

Nestle European Pension Fund (NEPF) - Institution for Occupational Retirement Provision
FSMA identification number 50.111
Rue de Birmingham 221 - 1070 Brussels

Identification data

- Address (professional, private)
- Mobile number (professional, private) or email address
- Employee number
- National number (if applicable)

Financial details

- Affiliation date
- Pension Plan (type, benefits, etc.)
- Beneficiaries (spouse pension, orphan's pension, ...)
- Personal contribution
- Bank account details

Personal details

- First/Last Name
- Birth date
- Gender
- Language
- Signature
- Nationality
- Marital status

Household composition

- Marriage or cohabitation type
- Partner : Name, birthdate, gender
- Child(ren): Name, birthdate, gender, number, dependent child(ren)

Health details

- Medical certificate illness/accident
- Start date of illness/accident
- End date of illness/accident
- % of employment (full time, part time)
- Duration of illness/accident

Employment

- Seniority data
- Start date
- Employer Name and the history
- Department Name + Identification Number of the department
- Contract type
- Career Interruption: start date, end date, % of employment
- % of employment (full time, part time)

- End of employment date
- End of employment reason
- Salary at 100%

Sensitive personal data:

Health details (duration of suspension of the employment contract for the work incapacity benefits)

e) The recipients of the Personal Data

Knowing Nestlé is established in many countries and that NEPF is a cross border pension fund, to be able to carry our activities, NEPF may transfer Personal Data of Plan Members and Beneficiaries to third parties if disclosure is consistent with the purposes of Data Processing, or if the Plan Members / the Beneficiaries give their consent hereto, if the Controllers are legally required to do so, or in relation to criminal investigations or other investigations by the government.

In the framework of the management and administration of the Pension Plans, Personal Data can be disclosed by the Controllers to, or can by processed by, amongst others:

- To a party as required or permitted by applicable law;
- To another company of the Nestlé group acting as a service provider or to external service providers (including :
    - Payroll service providers,
    - Benefit consultants,
    - Data hosting companies,
    - The internal auditor,
    - The compliance officer,
    - The appointed actuary,
    - The statutory auditor,
- Etc.

If the Personal Data are transferred to a Processor who processes this data on behalf of the Controllers, the Controllers will only use Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing is implemented in accordance with the GDPR and that the rights of the Plan Members and the Beneficiaries are protected. The Controllers shall conclude a written agreement with the Processor, containing at least the information required by the Legislation and Regulations concerning Data Protection. This agreement explicitly determines that the Processor can only process the Personal Data on the basis of written instructions from the Controllers and stipulates the guarantee of the Processor that the persons who he/she will authorise to process the Personal Data will respect the confidentiality of these data. Furthermore, the agreement explicitly stipulates whether the Processor is allowed to engage subcontractors (sub-processors) and if so, under which conditions.

f) Storage period

NEPF and the Sponsoring Undertakings will only keep the Personal Data and Sensitive Personal Data for the time needed for the relevant purposes, i.e. as long as NEPF and/or the Sponsoring Undertakings can have a legal responsibility or liability in the framework of the management and administration of the Pension Plans, taking into account the applicable statute of limitations. .
In principle, this means that the Personal Data are kept until:

- in case of payment of a one-off pension, ten years after the payment but not earlier than five years after the legal retirement age.
- in case of payment of a death or orphan lump sum: ten years after the payment;
- in case of payment of survivor's pensions and orphan's annuities: ten years after the payment of the latest annuity;
- in case of an individual transfer of the vested reserves: ten years after the legal retirement age.
- In case of payment of a disability pension: ten years after the payment of the last annuity.

However, if a longer statute of limitations would apply, the aforementioned retention periods will be adapted accordingly.

NEPF ensures that the Personal Data will be deleted, destroyed or anonymised after expiry of the abovementioned retention periods and takes the necessary measures to ensure that these Personal Data are also erased by the Processors who have these Data at their disposal. When Data is no longer required for any purpose, it will be securely deleted, destroyed or anonymized.

2) Data subject rights

Chapter III of the General Data Protection Regulation describes the rights of the Data Subjects. The Controllers shall take appropriate measures to provide any information and any communication referred to the Data Subjects' rights (articles 13 – 22) relating to Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. In that context, NEPF will provide:

- a start letter to the new Active Plan Members with the information required by law
- the information required by law concerning the Processing of Personal Data to the current Plan Members and Effective Beneficiaries;
- the information required by law concerning the Processing of Personal Data to the new Effective Beneficiaries together with the communication on the entitlement and payment of the death benefit by virtue of the Pension Plans;
- for every Data Subject (Deferred Plan Members excluded) this Data Privacy Policy on the local Intranet or web portal.
- For the Deferred Plan Members, the Data Privacy Policy is available on request.

Those rights are only applicable for the Personal Data of the Data Subject himself/herself, meaning that he/she cannot access the Personal Data of someone else.

NEPF shall provide information on any action taken on a request of a Data Subject as mentioned under a) to f) hereunder to the Data Subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. NEPF shall inform the Data Subject of any such extension within one month of receipt of the request,

together with the reasons for the delay. Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

The measures in question (providing information, rectification or erasure of Personal Data, transfer of data, etc.) shall be provided free of charge for the requesting Plan Member or Beneficiary. However, where requests from a Plan Member or a Beneficiary are manifestly unfounded or excessive, in particular because of their repetitive character, NEPF may either: a) charge a reasonable fee taking into account the administrative costs of providing the requested information or communication or taking the requested measure; or b) refuse to act on the request.

If NEPF does not take action on the request of the Data Subject, NEPF shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

To exercise the following rights (see points a) to f)), the data subjects can directly contact NEPF by email or by letter:

Nestlé European Pension Fund – Patrick Yot

Rue de Birmingham 221, 1070 Brussels (Belgium)

NEPF@be.nestle.com

a) Right of access by the data subject (article 15 GDPR)

The Data Subject has the right to obtain the following information:

- The purposes of the processing
- The categories of personal data concerned
- The recipients of the personal data
- The period for which the personal data will be stored
- The existence of the right to request access, erasure, modification or restriction
- The right to lodge a complaint with a supervisory authority
- From which source the personal data originate
- The appropriate safeguards relating to the transfer of Personal Data to a third country or an international organisation outside the EEA.

The Data Subject also has the right to obtain a description and copy of his/her Personal Data.

b) Right to rectification (article 16 GDPR)

The Data Subject has the right to obtain from NEPF without undue delay the rectification of inaccurate Personal Data concerning him or her.

c) Right to erasure (article 17 GDPR)

The Data Subject has the right to obtain the erasure of Personal Data when:

- The Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- There is no real reason for the Processing
- There is an unlawfully Processing of Personal Data
- The Personal Data have to be erased for compliance with a legal obligation

NEPF is responsible to make sure that the request for erasure of the Personal Data was taken into account by the processors.

The right to erasure can't be applied when there is a legal obligation to process Personal Data or when there is a contractual obligation.

d) Right to restriction of Processing (article 18 GDPR)

The Data Subject should have the right to obtain the restriction of Processing:

- During a limited period to verify the accuracy of the Personal Data
- When the processing is unlawful
- When there is no need anymore to process Personal Data.

e) Right to data portability (article 20 GDPR)

The Subject Data can ask to transfer the Processing of his/her Personal Data to another recipient in charge of processing.

f) Right to object (article 21 GDPR)

Where Personal Data are processed for direct marketing purposes, the Data Subject has the right to object at any time to processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

NEPF ensures that Personal Data are not and will not be used for such purposes.

3) Data protection measures

At the time of the determination of the means for Processing and at the time of Processing itself, the Controllers must implement measures which are designed to implement data-protection principles. The Controllers must implement measures for ensuring that by default, only Personal Data which are necessary for each specific Purpose of the Processing are processed.

NEPF has taken appropriate technical and organizational security measures to protect your Personal Data against unlawful or unauthorized processing. This includes, without being limited to:

- The provision of secure operating systems and processes to ensure that your Personal Data is only accessible to Nestlé employees, agents and contracted personnel on a need-to-know basis and according to industry standards for the security and protection of personal data;

- All Authorised Users are obliged to do the necessary to comply with this Policy in order for NEPF and the Sponsoring Undertakings, as joint Controllers, to comply with the Legislation and Regulations concerning Data Protection;
- The encryption of Personal Data ;
- Personal Data are shared between recipients via a Sharepoint with limited access or when sent by mail protected by a password;
- Personal Data are shared after identity checks of the Plan Member ;
- Raising awareness regarding the GDPR among the stakeholders of NEPF ;
- The cupboard where paper information might be stored are locked ;
- In case of technical/physical incident, ability to restore the availability and access to Personal Data;
- Process for regularly testing, assessing and evaluating the effectiveness of measures ensuring the security of processing;
- An authentication to the Nestlé account is required. It is a system to check the identity of the employee. It prevents unauthorised access.

4) Data Breach Policy

Legal context

Notification to the Supervisory Authority

If at Breach has or is likely to have significant negative consequences for the protection of the Personal Data involved, it should be reported to the Data Protection Authority.

The Processor must inform NEPF and/or a Sponsoring Undertaking within 36hours of any incident related to information security and of any Breach.

NEPF will then initiate an investigation to verify the nature of the incident, the type of data involved, whether Personal Data is involved, and if so, which Plan Members and Beneficiaries are concerned. This investigation will show whether or not it constitutes a Breach.

If there is a Breach, NEPF must then notify the Breach to the Data Protection Authority within 72 hours maximum after the incident. The notification must include:

- The reason of the delay if more than 72hours
- Description of the nature of the data breach (Who/what= categories of people and data concerned, How many = the number)
- Contract details of the Controller
- Description of the likely consequences
- Solutions

That information can be provided at different moments but always before the deadline of 72hours.

If the Breach has an impact in different member states, then NEPF shall inform all supervisory authorities.

Incidents linked to Personal Data that do not have an impact for the rights and freedoms of individuals do not need to be reported to the supervisory authority.

Notification to the individuals

When necessary according to article 34.3 GDPR, the Data Subjects concerned will be informed of the Breach with the following details:

- Description of the nature of the data Breach
- Contact details of the Controller
- Description of the likely consequences
- Solutions

Data breach and risks

Several factors can be used to see if the Breach leads or not to a risk for the Data Subject:

- The nature, sensitivity and volume of personal data
- Ease of identification of individuals
- Severity of consequences for individuals
- Special characteristics of the individuals
- The number of affected individuals
- Special characteristics of the Data Controller

Data Breach record

The Controllers shall document any Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall enable the Data Protection Authority to verify compliance with this Article.

Template – Data Breach Notice

To notify the incident, the Processor must use the following template and send it to NEPF. When required, NEPF must send the documents to the Data Protection Authority. The Controllers can directly fill in the template if they notice a Breach.

Regarding the notification to the Plan Members and Beneficiaries, the communication will depend on several factors (population concerned, data impacted, level of impact and so on). In other words, depending on situations, a large scale or a personal communication can be made.

Nestle European Pension Fund (NEPF) - Institution for Occupational Retirement Provision
FSMA identification number 50.111
Rue de Birmingham 221 - 1070 Brussels

Data Breach Notification

In the event of a breach to protect personal data against accidental or unlawful destruction or accidental loss, alteration, misuse, unauthorised disclosure/access or all other unlawful forms of Processing, please describe the:

- NEPF Controller(s) affected by the breach:

  ……..
- Nature of the breach, including the categories and number of Data Subjects and data records concerned:

  ……..
- Facts surrounding the breach:

  ……..
- Date of discovery of the breach:

  ……
- Suspected date of occurrence of the breach:

  ……..
- Consequences and effects of the breach:

  ……..
- Identity and contact details of the data protection officer, if any, or another contact point where more information can be obtained:

  ……..
- Measures proposed or taken to mitigate the possible adverse effects of breach and address it:

  ……..

Supplier

Name:

Title:

Date:

Signature: