skills workflow

GDPR

May, 2025

Bruno Moscão CTO
bruno@skillsworkflow.com
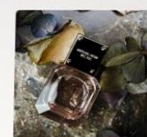
Agenda

Optimize every corner of your agency

1 **Personal Privacy**

2 **User Rights**

3 **Controls and Notifications**

4 **Transparent Policies**

5 **IT and Training**

Transform your agency. Make it an oasis of creativity and champion of productivity. Why use people to do tedious work software can do? Let computers do repetitive tasks and predict problems. Then, leverage human judgement to make the best decisions.

1. Personal Privacy

Personal Privacy Rights

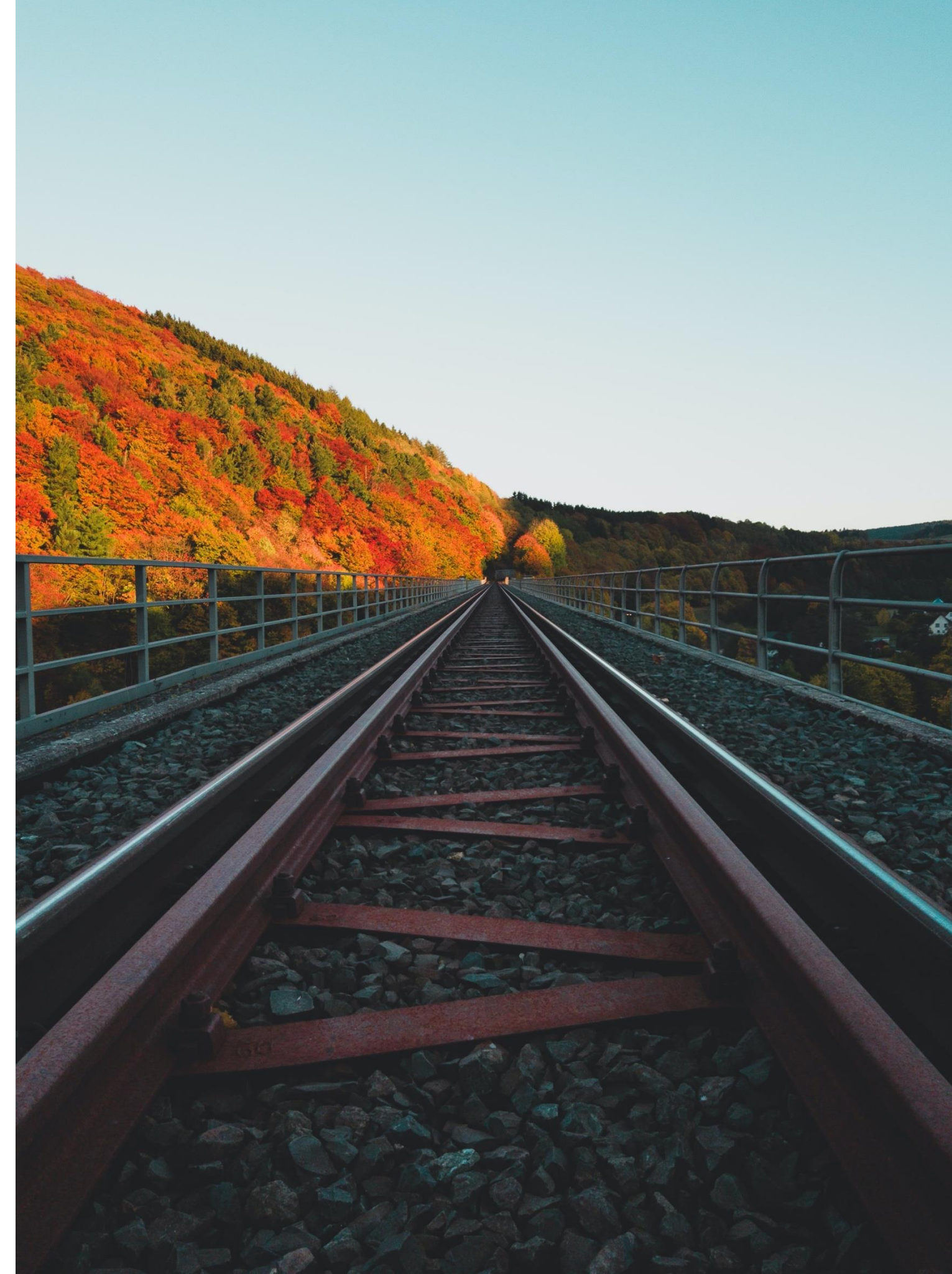Individuals have the right to Manage their Personal Data

Access Personal Data

Correct Errors in Personal Data

Erase Personal Data

Object to Processing of Personal Data

Export Personal Data

Personal Identifiable Information

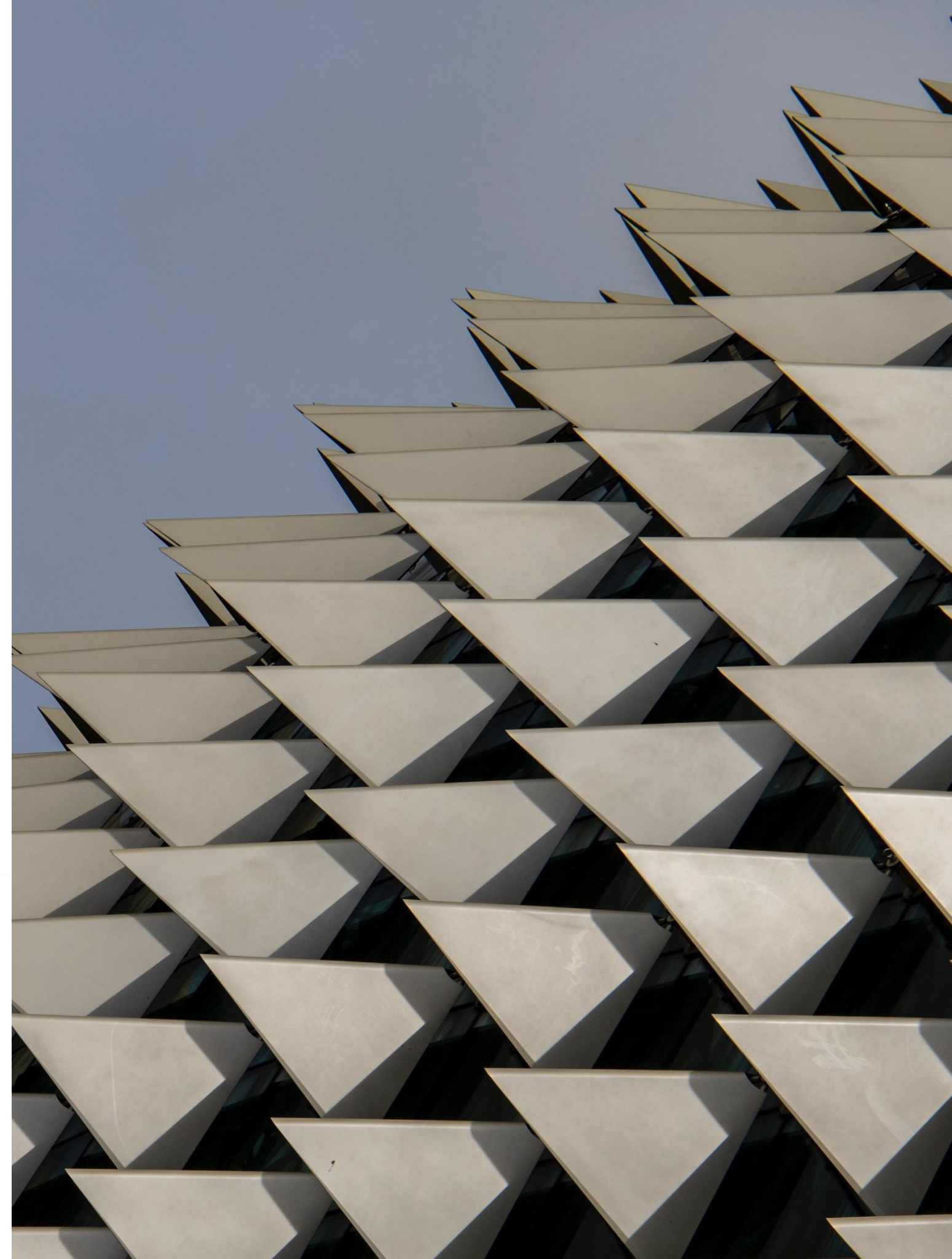What's Stored

Usernames are created for each Employee

Company's Emails are stored for each Employee

Birth Date is optional for each Employee

Taxpayer Number is optional for each Employee

Avatar is an image that the Employee chooses

Phone Number is optional for each Employee

Personal Identifiable Information

What is Personal Identifiable Information used for

Usernames are used to map to ERP, HR or AD

Company's Emails are used to send Notifications

Birth Date is used only to congratulated on Birthdays

Taxpayer Number is used for Reporting purposes

The Avatar is way for the User identify him/herself
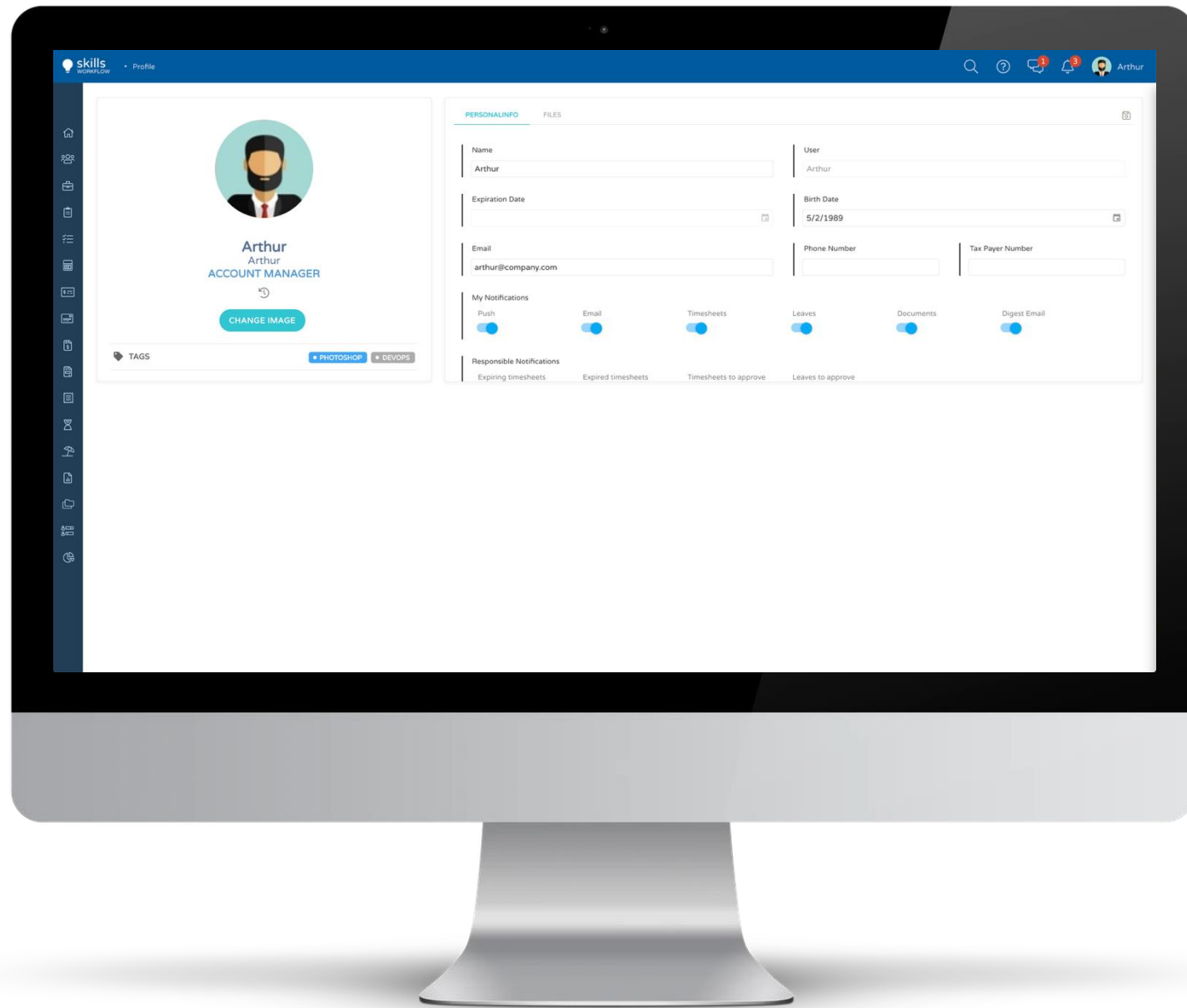
Phone Number is the User contact in the Company

2. User Rights

Access Erase and Correct

Tools to Comply to Requirements

Users can see their Personal Identifiable Information

Can edit PII to make amends or remove it

Companies may decide to have no PII in the system

Users maybe restricted from adding PII to system

Personal Data Processing

Personal Identifiable Data is never processed

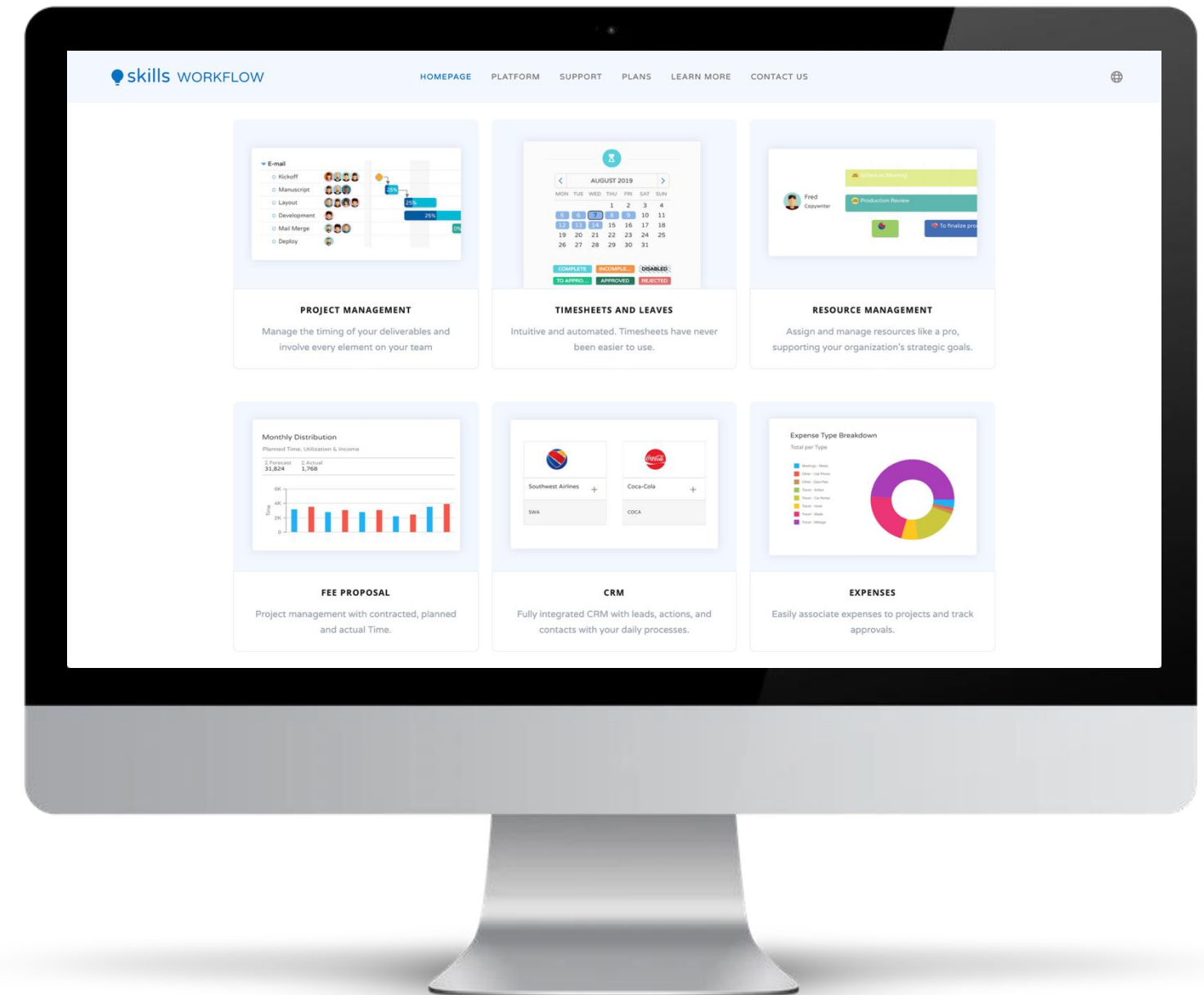PII is not processed in the system

Some of it is used to link tools (e.g. AD, ERP)

Predictions in the system never use PII

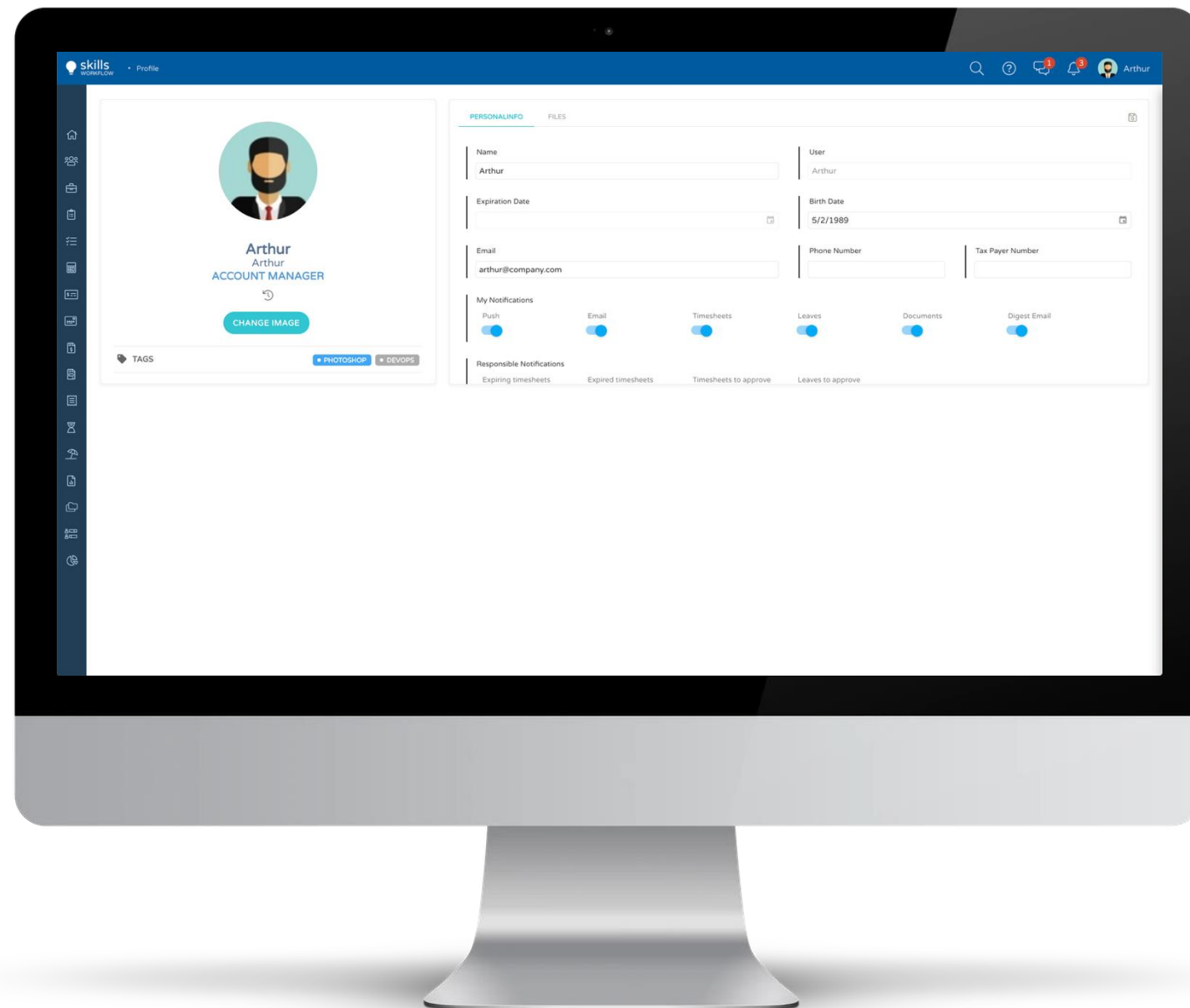Only historical data is used to suggest actions

Birth Date may be used to detect Birthdays

Taxpayer, Username, Email used to link tools

Personal Data Export

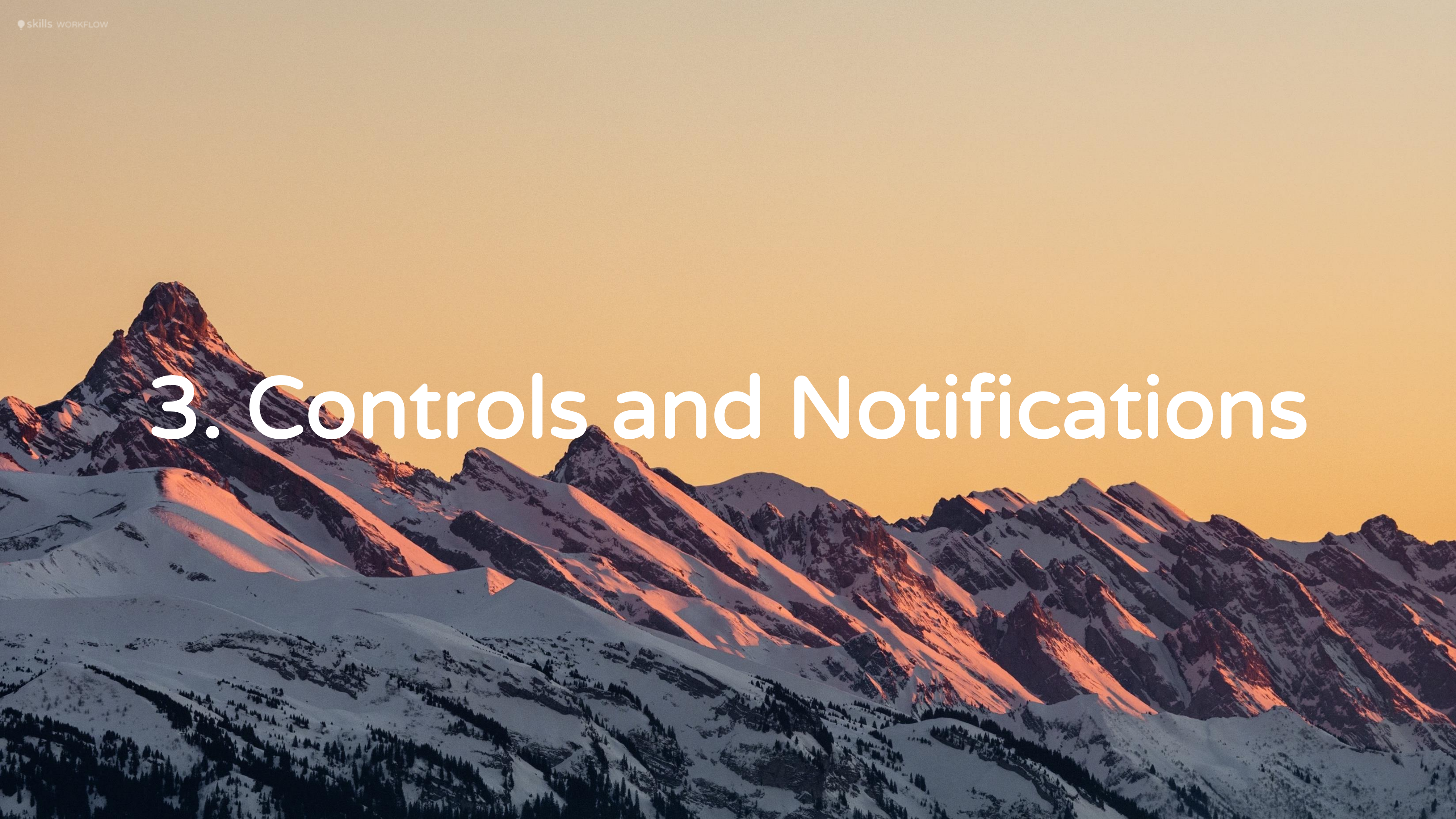How to export Personal Identifiable Data

Users may print their Profile

There are Dashboards to export PII

Users may use these tools in self-service mode

Company may export individual PII and send to User

Access controls prevent unauthorized access

3. Controls and Notifications

Personal Data

Protect, Notify, Process and Obtain Consent on Personal Data

Use of Appropriate Security

Notify on Personal Data Breaches

Obtain Consent on Processing Data

Keep records on Data Processing

Humanized by Skills Workflow

SOC I & II

Delloite performs audit on SSAE

Annually Skills Workflow is audited by Deloitte

Audit also includes Security

Controls are in place to assure Data is Secure

Data is Encrypted in transit and at rest

Audit logs are kept on who changes Data and when

If Breached, there's a procedure inform Clients

Craft with ♥ on Skills Workflow

Securing Data

Channels and Encryption

Data is encrypted both at Rest and in Transit

In transit is HTTPS up to TLS 1.2

PII when exported to files is PGP encrypted

At Rest for SQL Server using TDE Encrypted

At Rest for Cosmos & Storage using AES-256

Humanized by Skills Workflow

Breaches
Procedures and Communication

When data is Breached there's a simple process

Every Key User of the breached Tenant is contacted

Contacts for Key Users per Instance are kept

Data is Encrypted in transit and at rest in Helpdesk

The Head of Security is Responsible for this Process

Craft with 💗 on Skills Workflow

Consent on Data
Users grant consent to Data

Users grant the consent to the Company

PII changes are audited on who and when

Users can key in their own PII (self service)

Company may fill in the data if allowed by User
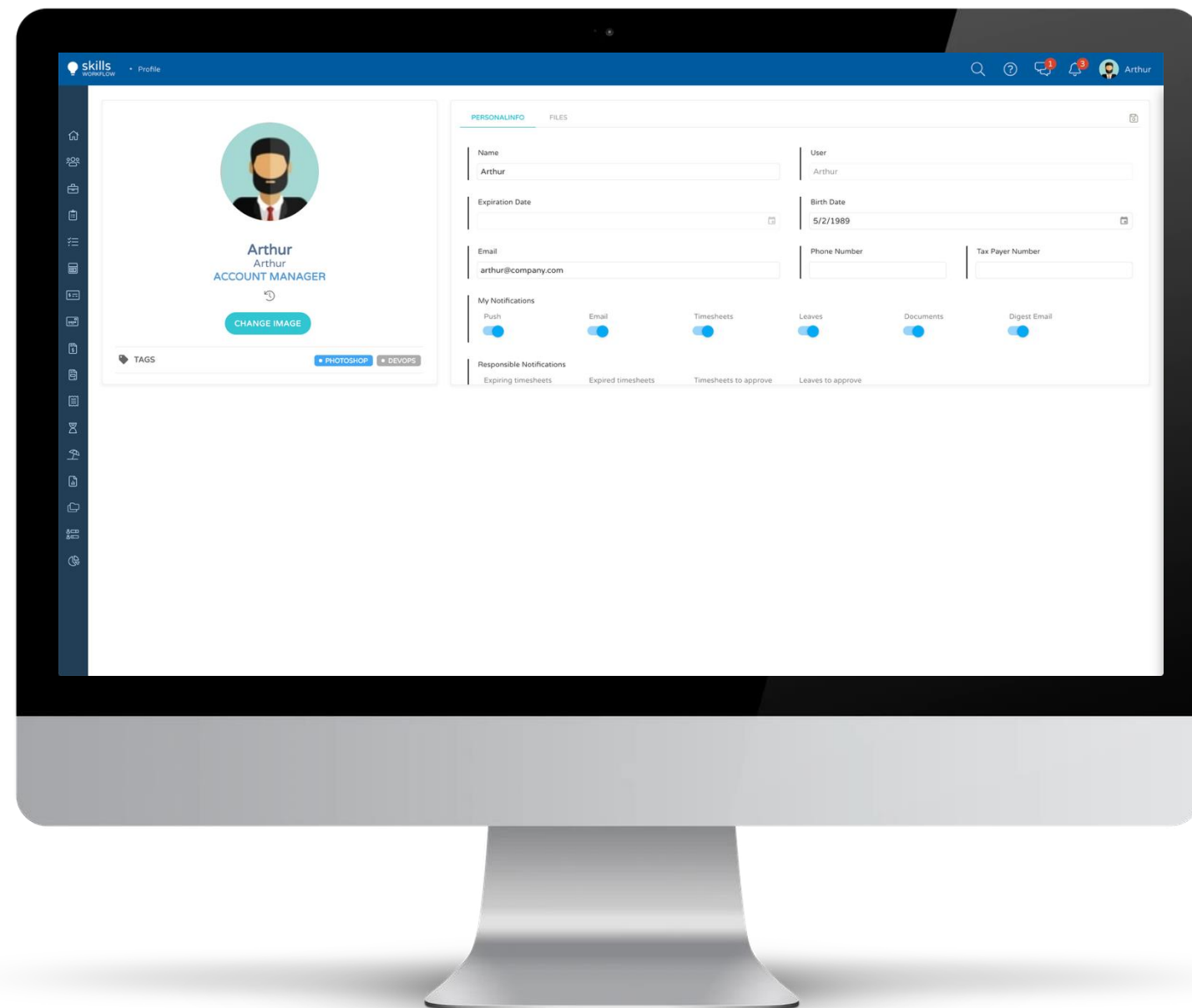
Data Processing
How PII is processed

PII is never processed by the system

The Birth Date is used for announce Birthdays

4. Transparent Policies

Transparent Policies

Provide Notice, Outline Purposes, Define Policies on Personal Data

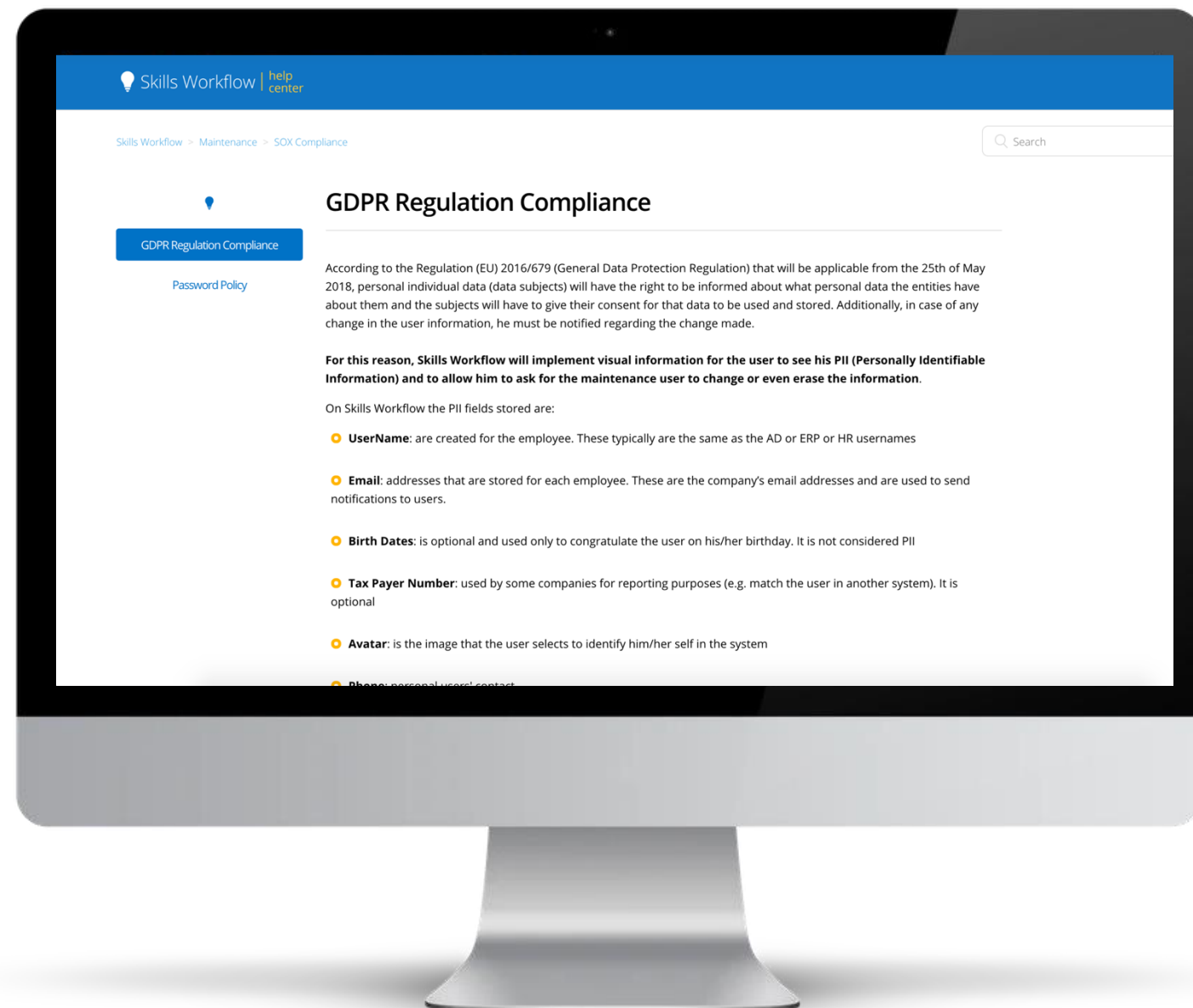Data is shown clearly and transparently

Clear Notice on data collection

Processing purposes and Use Cases

Detection and Deletion Policies

Processing Purposes
Documented on Help Centre

Details are stated in the Help Centre

Links to a from the User Profile to Help are provided

Help Centre explain what each field means

Education is also on not to expose PII

PII potential usage is explained in detail

Clear Notice
Communication

Users are clearly informed when changing PII

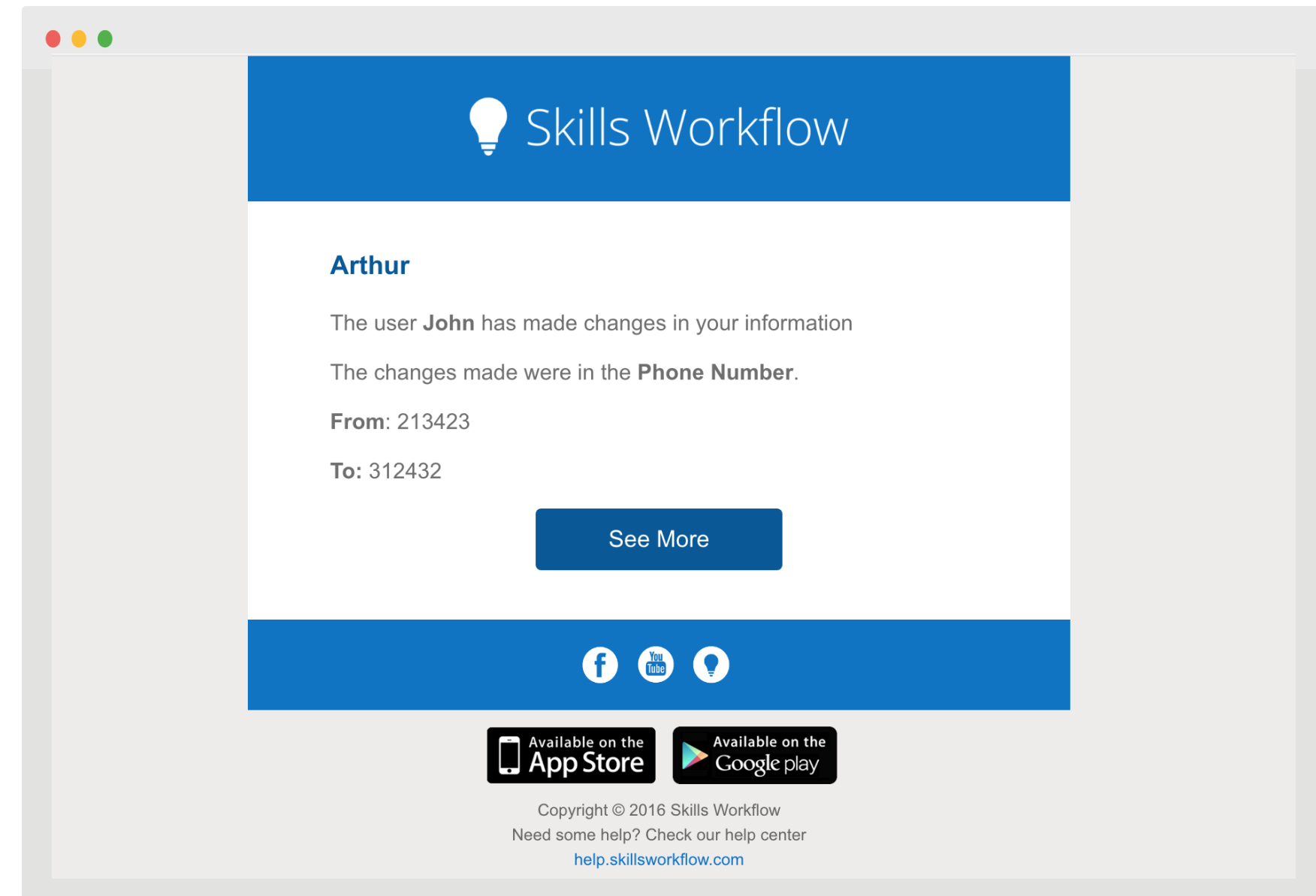Automaticatic changes are also informed

Automatic Data is Username, AD User, Email

After data is changed, User needs to confirm

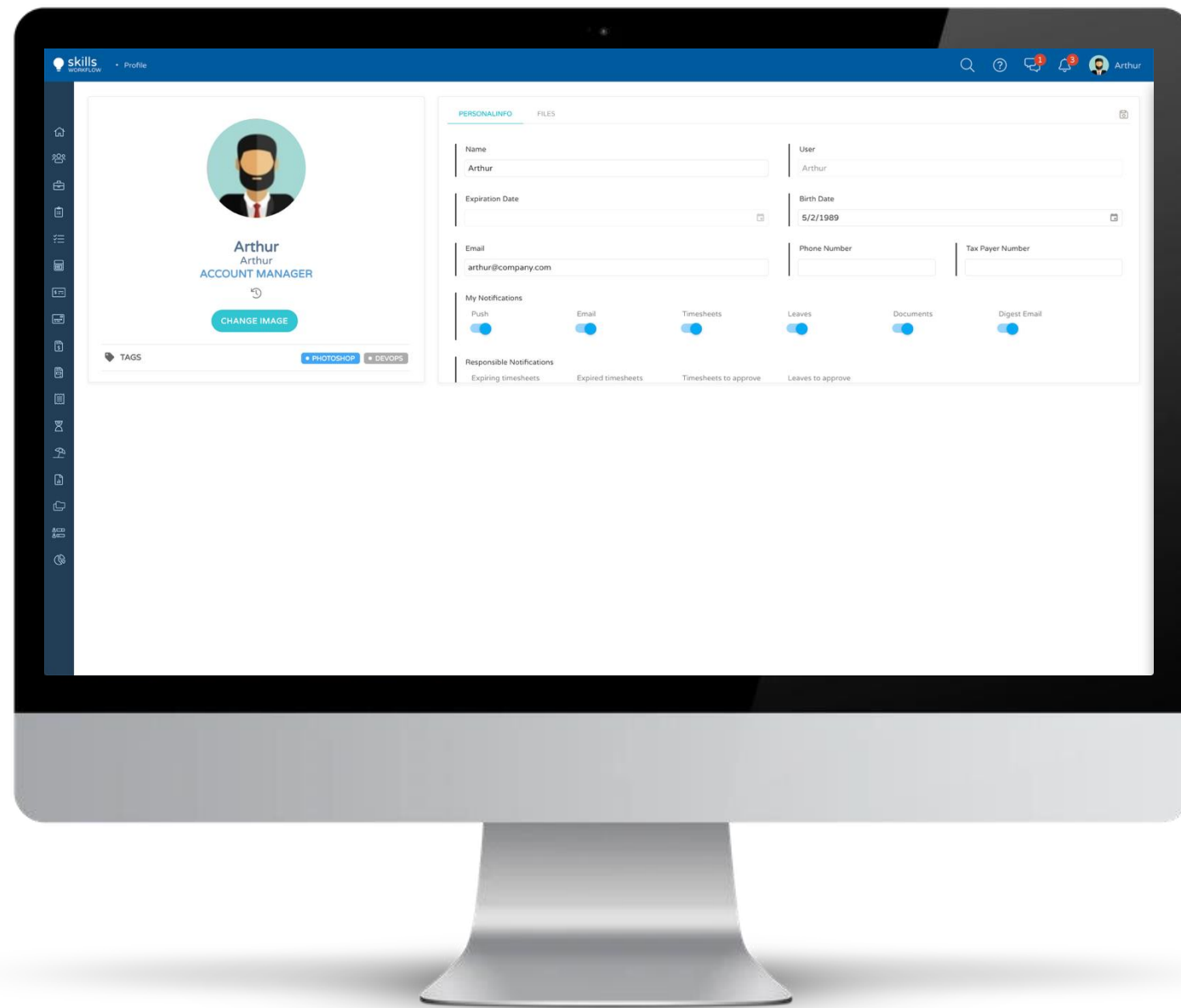The User is Notified by email and Push

Storage is complete on User's confirmation

Audit is kept on who, when and what changed

Retention Policy
Terminated Users and Company Termination

When User is terminated, the User is inactivated

Data is only eliminated if User demands it

Company may scramble information if desired

Data scrambling includes Profile and Audit logs

If Company is terminated, data is kept for 35 days

After 35 days, the data is deemed unrecoverable

5. IT and Training

# IT and Training

Personal Identifieable Information

1 **IT is Trained on how to answer Users**
PII, GDPR, Breachs, Precautions, Rights, Tools

2 **Audit and Data Policies**
IT is educated on what is in Audit and how Data is stored and kept

3 **Data Protection Officer**
The Company has to clear specify who is the Data Protection Officer

4 **Microsoft Azure Compliance**
IT learns what is the role of Microsoft in PII and data

Humanized by Skills Workflow

IT Training

Answering Users questions and proving Tools

IT is trained on how to answer Users' questions

IT can explain on how to extract data

And IT tutors Users on the Right to be Forgotten

This Document is part of the IT Training

The Document is public to anyone
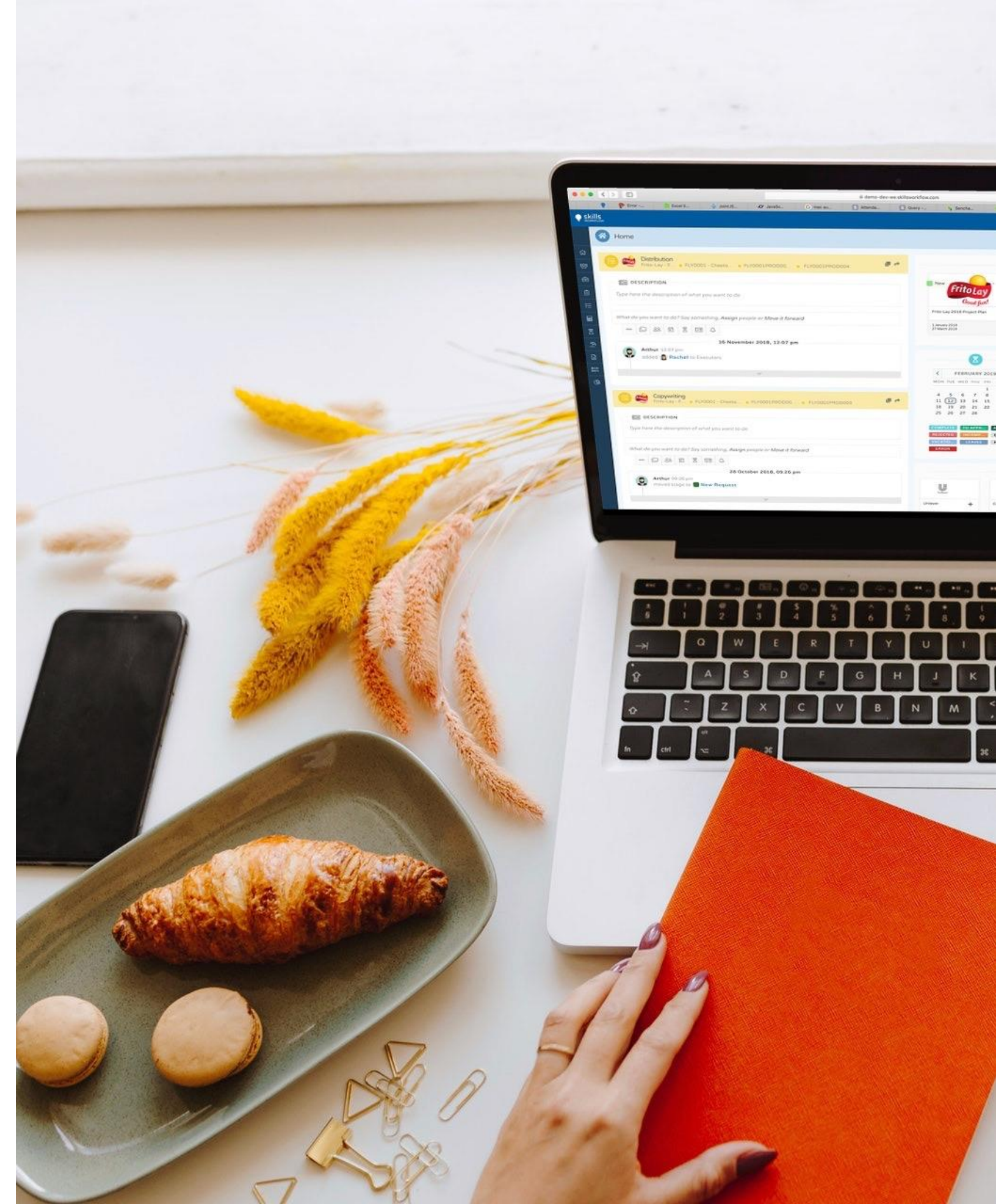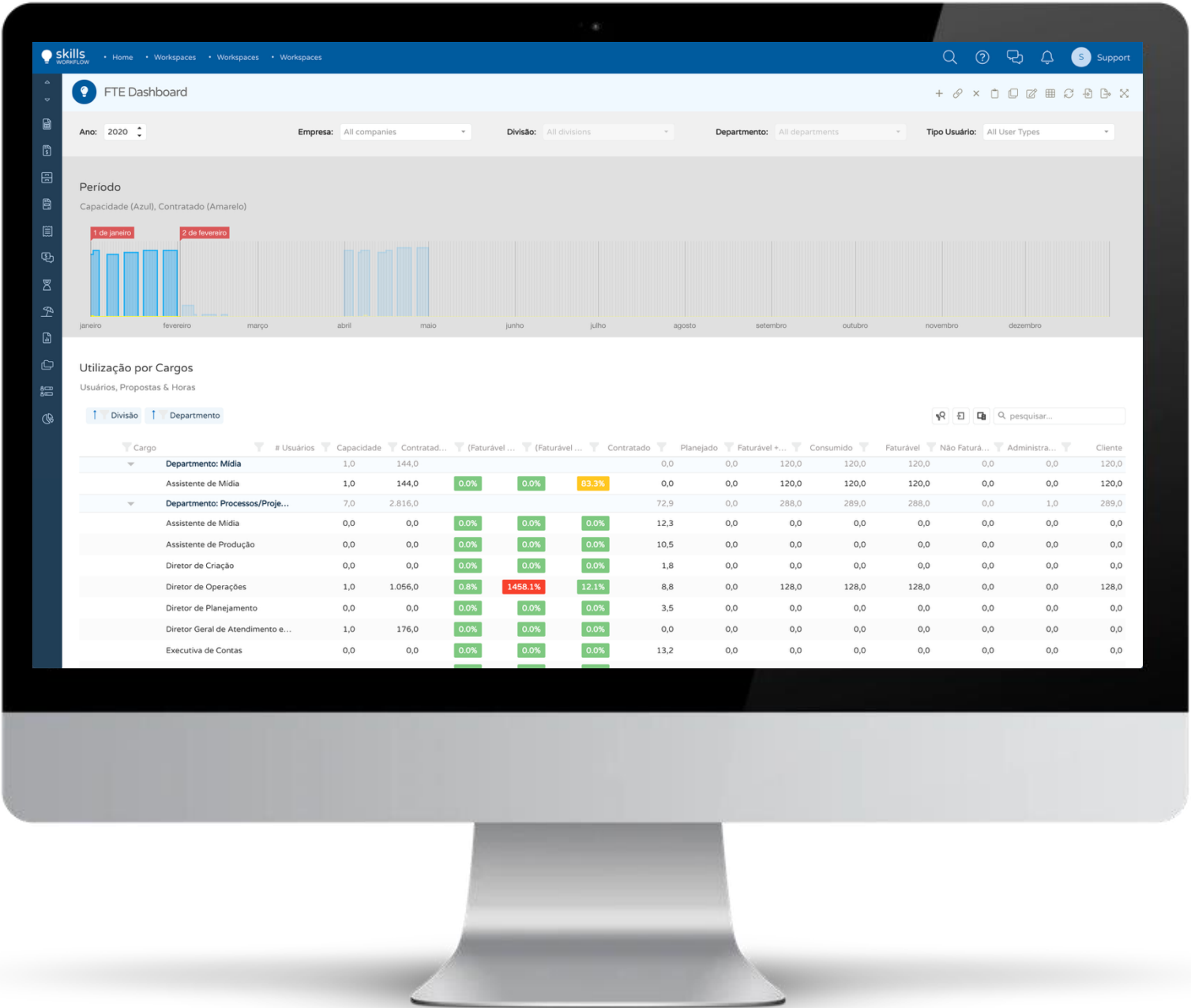
Reporting
Audit and Dashboards

There is a set of Dashboards for GDPR

The data is controlled by User Access

Audit is also shown in the Dashboards

Audit shows who, what and when PII was edited

IT shows the User Profile as the center point

Compliance

It's the Client's Company Responsibility

Compliance is enforced by the Client

The Tools exist and are in Place

IT is 1st line Support, trained to ensure Compliance

There's Consent, Notification, Rights and Extraction

Everything is transparent and in line with GDPR

Helpdesk and Help Centre provide 2nd line Support

Azure also helps with Retention and Deletion

There are also tools to determine Compliance Scores

Data Protection Officer

The Company is demanded, by GDPR, to have one

The DPO is the responsible for GDPR at the Client

DPO receives training like IT

This Document is also a reference for the DPO

DPO should check the Company's score on GDPR

DPO must handle all systems (not just Skills Workflow)

Thank You!

Bruno Moscão CTO
bruno@skillsworkflow.com

Craft with ♥ on Skills Workflow