Presented by Yann Jaffrennou (H00334786)

Tutored by Manuel Maarek

Course F21IM

Spoiler: it's not that bad

IT MASTER CLASS

A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

"OWNER, FOUNDER OR MANAGER OF AN INTERNET BASED BUSINESS"

Fall 2019

INTRODUCTION: OBJECTIVES OF THE CLASS

- Being GDPR compliant while creating new solutions
- Understand GDPR and its implications
- Detect eventual “hot spots”
- Have a few tips and pre-made solutions

INTRODUCTION: MENU

- Part. 1: GDPR
- Part. 2: Data
- Part. 3: Services
- Part. 4: Use of External Services (Third party)

A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

PART. 1: GDPR

1. GDPR: WHAT IS GDPR?

Global, “first layer”

European laws

GENERAL DATA PROTECTION REGULATION

Defines everything you can/cannot/have to do

Effects

Cookies | Emails | Terms of use | Boxes to check

GDPR → Data → Services → External Services

1. GDPR: WHAT IS GDPR?

ACCORDING TO THE GDPR (ART. 1)

- "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data"

- "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"

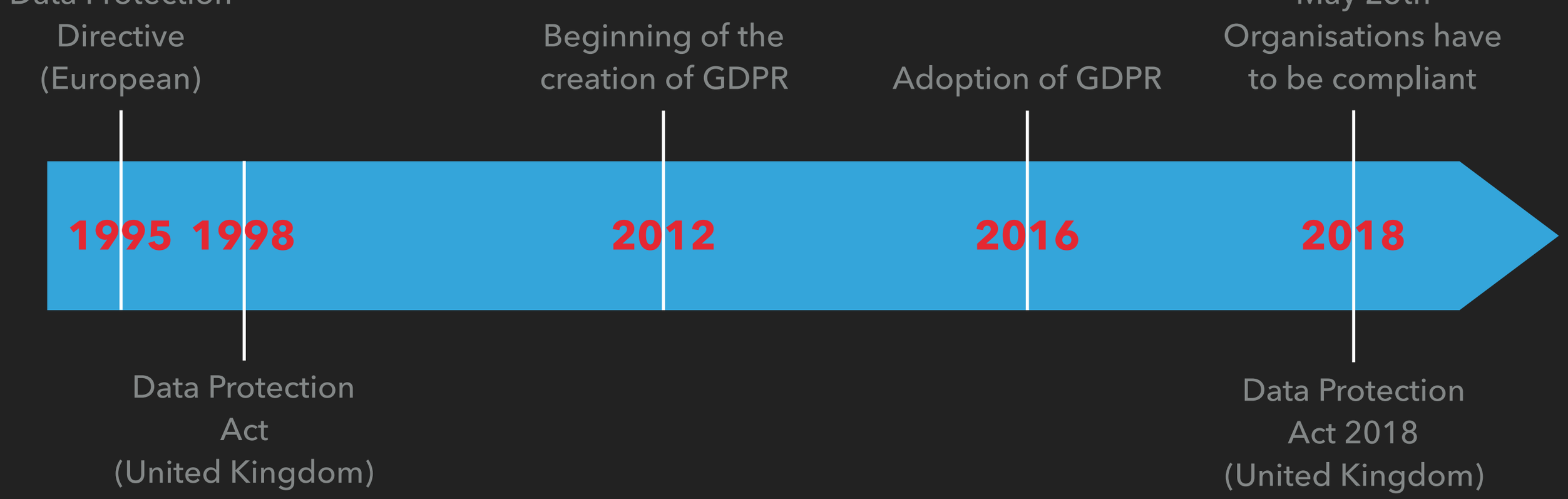
gdpr-info.eu (Official GDPR website)

1. GDPR: TERRITORIAL SCOPE

ACCORDING TO THE GDPR (ART. 3)

- "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the [European] Union, regardless of whether the processing takes place in the Union or not"

1. GDPR: HISTORICAL AND LEGAL CONTEXT



"THE DATA PROTECTION ACT 2018 IS THE UK'S IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR)" – WWW.GOV.UK
IT "MAKES PROVISION" AND "SUPPLEMENTS" – WWW.LEGISLATION.GOV.UK

1. GDPR: DIALOG WITH ORGANISATIONS (ART. 37–39, 51)

ORGANISATION

DATA PROTECTION OFFICER (DPO)

Represents the organisation regarding data privacy

GDPR

SUPERVISORY AUTHORITY

Responsible for the application of the GDPR

France: CNIL

UK: ICO

Liechtenstein: Data Protection Office

Ireland: Data Protection Commissioner

1. GDPR: THE PRICE TO PAY

ACCORDING TO THE GDPR (ART. 83)

- "[…] be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"

- Google: 30 000 000£
- Facebook: 500 000£ (Cambridge Analytica consequences)
- Uber: 350 000£

1. GDPR: DEFINITIONS

"'PERSONAL DATA' MEANS ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON ('DATA SUBJECT'); AN IDENTIFIABLE NATURAL PERSON IS ONE WHO CAN BE IDENTIFIED, DIRECTLY OR INDIRECTLY, IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, AN IDENTIFICATION NUMBER, LOCATION DATA, AN ONLINE IDENTIFIER OR TO ONE OR MORE FACTORS SPECIFIC TO THE PHYSICAL, PHYSIOLOGICAL, GENETIC, MENTAL, ECONOMIC, CULTURAL OR SOCIAL IDENTITY OF THAT NATURAL PERSON"

GDPR, Art. 4

1. GDPR: DEFINITIONS

> "'PROCESSING' MEANS 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"

GDPR, Art. 4

1. GDPR: DEFINITIONS

"'FILING SYSTEM' MEANS ANY STRUCTURED SET OF PERSONAL DATA WHICH ARE ACCESSIBLE ACCORDING TO SPECIFIC CRITERIA, WHETHER CENTRALISED, DECENTRALISED OR DISPERSED ON A FUNCTIONAL OR GEOGRAPHICAL BASIS"

GDPR, Art. 4

1. GDPR: DEFINITIONS

> "'CONTROLLER' MEANS THE NATURAL OR LEGAL PERSON, PUBLIC AUTHORITY, AGENCY OR OTHER BODY WHICH, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES AND MEANS OF THE PROCESSING OF PERSONAL DATA; WHERE THE PURPOSES AND MEANS OF SUCH PROCESSING ARE DETERMINED BY UNION OR MEMBER STATE LAW, THE CONTROLLER OR THE SPECIFIC CRITERIA FOR ITS NOMINATION MAY BE PROVIDED FOR BY UNION OR MEMBER STATE LAW"

GDPR, Art. 4

1. GDPR: DEFINITIONS

> "'PROCESSOR' MEANS A NATURAL OR LEGAL PERSON, PUBLIC AUTHORITY, AGENCY OR OTHER BODY WHICH PROCESSES PERSONAL DATA ON BEHALF OF THE CONTROLLER"

GDPR, Art. 4

1. GDPR: SUMMARY

- Does not only concern data on hard drives (out of the scope of this Master Class)
- Everybody processes personal data
- Punishes severely
- Concerns “only” personal data
- More specific laws exist in countries

A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

PART. 2: DATA

2. DATA: MORE ABOUT PERSONAL DATA

Regular personal data

Name
Date of birth
Pseudonym
City of living
Address
Phone number
Age
Location data

Sensitive personal data

Religious/Philosophical beliefs
Ethnic/Racial origin
Sexual orientation
Political opinions

PERSONAL DATA

Genetic data

DNA sample
RNA Analysis
Biological sample

Biometric data

Facial images
Fingerprints
Voice recognition
Iris scans

Data concerning health

Electrocardiograms
Heart rates
Sleep tracking
Running speed

2. DATA: GDPR SAYS DATA SHALL BE

"PROCESSED LAWFULLY, FAIRLY AND IN A TRANSPARENT MANNER IN RELATION TO THE DATA SUBJECT ('LAWFULNESS, FAIRNESS AND TRANSPARENCY')"

GDPR, Art. 5

2. DATA: GDPR SAYS DATA SHALL BE

"COLLECTED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES AND NOT FURTHER PROCESSED IN A MANNER THAT IS INCOMPATIBLE WITH THOSE PURPOSES"

GDPR, Art. 5

2. DATA: GDPR SAYS DATA SHALL BE

"ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY IN RELATION TO THE PURPOSES FOR WHICH THEY ARE PROCESSED ('DATA MINIMISATION')"

GDPR, Art. 5

2. DATA: GDPR SAYS DATA SHALL BE

"ACCURATE AND, WHERE NECESSARY, KEPT UP TO DATE; EVERY REASONABLE STEP MUST BE TAKEN TO ENSURE THAT PERSONAL DATA THAT ARE INACCURATE, HAVING REGARD TO THE PURPOSES FOR WHICH THEY ARE PROCESSED, ARE ERASED OR RECTIFIED WITHOUT DELAY ('ACCURACY')"

GDPR, Art. 5

2. DATA: GDPR SAYS DATA SHALL BE

"KEPT IN A FORM WHICH PERMITS IDENTIFICATION OF DATA SUBJECTS FOR NO LONGER THAN IS NECESSARY FOR THE PURPOSES FOR WHICH THE PERSONAL DATA ARE PROCESSED"

GDPR, Art. 5

2. DATA: GDPR SAYS DATA SHALL BE

> "PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF THE PERSONAL DATA, INCLUDING PROTECTION AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING AND AGAINST ACCIDENTAL LOSS, DESTRUCTION OR DAMAGE, USING APPROPRIATE TECHNICAL OR ORGANISATIONAL MEASURES ('INTEGRITY AND CONFIDENTIALITY')"

GDPR, Art. 5

2. DATA: GDPR SAYS...

"THE CONTROLLER SHALL BE RESPONSIBLE FOR, AND BE ABLE TO DEMONSTRATE COMPLIANCE WITH, PARAGRAPH 1 ('ACCOUNTABILITY')"

GDPR, Art. 5

2. DATA: CAN YOU PROCESS THIS DATA?

IS IT A SPECIAL KIND OF PERSONAL DATA?

NO

YES

IS IT NEEDED TO PROVIDE YOUR SERVICES?

IS THERE ANY OTHER SOLUTION?

SHOULD NOT BE REQUIRED
ASK FOR CONSENT

CAN BE REQUIRED
EXPLAIN THE USE OF IT

READ THE TEXTS
CONTACT A SUPERVISOR

CHOOSE THE
OTHER SOLUTION

MAKE SURE YOUR DATA IS SECURED. INFORM THE USER. DO NOT KEEP IF NOT NEEDED. KEEP FRESH.

2. DATA: CONSENT (ART. 7)

- Be able to prove that the data subject has consented
- When asking for consent, it must be clearly distinguishable
- Consent is not freely given if it is required to access a service, but this service can be provided without it
- Consent must be as easy to withdraw as to give

2. DATA: DEFINITIONS

> "'PSEUDONYMISATION' MEANS THE PROCESSING OF PERSONAL DATA IN SUCH A MANNER THAT THE PERSONAL DATA CAN NO LONGER BE ATTRIBUTED TO A SPECIFIC DATA SUBJECT WITHOUT THE USE OF ADDITIONAL INFORMATION, PROVIDED THAT SUCH ADDITIONAL INFORMATION IS KEPT SEPARATELY AND IS SUBJECT TO TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THAT THE PERSONAL DATA ARE NOT ATTRIBUTED TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON"

GDPR, Art. 4

2. DATA: EXAMPLE OF K-ANONYMISATION

PERSONAL DATA

Name	Age	City
C. Kent	18	Paris
T. Stark	21	London
F. Type	32	Bordeaux
T. Max	24	Manchester
T. Cook	45	Dubai
E. Musk	38	Abu Dabi

2-ANONYMISED PERSONAL DATA

Name	Age	Country
-	20-35	France
-	20-25	UK
-	20-35	France
-	20-25	UK
-	35-50	UAE
-	35-50	UAE

MORE COLUMNS = LESS DETAILS

NOTE: THIS IS TO EXPLAIN THE METHODS USED FOR ANONYMISING PERSONAL DATA. HERE, DELETION OF NAME IS SUFFICIENT. THERE IS OBVIOUSLY MORE THAN ONE 18 YEARS OLD HUMAN LIVING IN PARIS: EACH ROW DOES NOT PERMIT TO IDENTIFY ONE SINGLE INDIVIDUAL. FOR K-ANONYMISATION, K MUST BE STRICTLY GREATER THAN 1

2. DATA: EXAMPLE OF K-ANONYMISATION

PERSONAL DATA

Name	Age	City
C. Kent	18	Paris
T. Stark	21	London
F. Type	32	Bordeaux
T. Max	24	Manchester
T. Cook	45	Dubai
E. Musk	38	Abu Dabi

2-ANONYMISED PERSONAL DATA

Name	Age	Country
-	20-35	France
-	20-25	UK
-	20-35	France
-	20-25	UK
-	35-50	UAE
-	35-50	UAE

MORE COLUMNS = LESS DETAILS

IMPORTANT: ANONYMISED DATASETS SHOW TRENDS. IF ALL THOMAS LIVING IN PARIS EARN EXACTLY 30K€ PER YEAR, IT IS NOT CONSIDERED AS PERSONAL DATA.

2. DATA: EXAMPLE OF PSEUDONYMISATION

PERSONAL DATA

Name	Age	City
C. Kent	18	Paris
T. Stark	21	London
F. Type	32	Bordeaux
T. Max	24	Manchester
T. Cook	45	Dubai
E. Musk	38	Abu Dabi

PSEUDONYMISED PERSONAL DATA

ID	Age	City
19375	18	Paris
19405	21	London
71849	32	Bordeaux
64473	24	Manchest
47295	45	Dubai
20563	38	Abu Dabi

NOTE: WITHOUT THE ID COLUMN, THIS PSEUDONYMISED DATASET IS ANONYMISED AS EXPLAINED IN THE BOTTOM NOTE OF PREVIOUS SLIDE. A PSEUDONYMISED DATASET WITHOUT PSEUDONYMS IS BY DEFINITION ANONYMISED

2. DATA: NOTE ON EMPLOYEE DATA BREACH

- Regarding GDPR, you (the company) are responsible
  - If the employee had to access the data for his work, you can sue him/her (Make sure to have some professional secret clauses about “confidential information” in your contracts of employment)
- If the employee did not need this access, it is considered as a security breach. You are fully responsible: secure your data and manage access!!!

2. DATA: A FEW ADVICES

- Use pseudonymisation as much as you can (isolation)
- Refer to Art. 6 to know if you can process some data
- Use APIs (makes it easier to change data structures)
- Build micro-services architectures (security by design)
- Do not let your developers access personal data (avoid employee breach)
- Use samples to test your services
- As soon as some data is old, anonymize it (Art. 11)
- Ask for consent

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address
- Generic Email address (contact@hw.ac.uk)
- Address
- Name and Address
- Name and 4 last digits of credit card
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk)
- Address
- Name and Address
- Name and 4 last digits of credit card
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address
- Name and Address
- Name and 4 last digits of credit card
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address
- Name and 4 last digits of credit card
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card ✓
- Receipt with date, time and last 4 digits of credit card
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card ✓
- Receipt with date, time and last 4 digits of credit card ✗
- Web cookie
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card ✓
- Receipt with date, time and last 4 digits of credit card ✗
- Web cookie ✓
- Company name and website
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card ✓
- Receipt with date, time and last 4 digits of credit card ✗
- Web cookie ✓
- Company name and website ✗
- Pay records with gender and age

PRACTICE: IDENTIFY PERSONAL DATA

- Personal Email address ✓
- Generic Email address (contact@hw.ac.uk) ✗
- Address ✗
- Name and Address ✓
- Name and 4 last digits of credit card ✓
- Receipt with date, time and last 4 digits of credit card ✗
- Web cookie ✓
- Company name and website ✗
- Pay records with gender and age ✓

PRACTICE: WHAT TABLE IS K-ANONYMIZED?

Name	Age	Country
-	20-25	France
-	20-25	UK
-	30-35	France
-	30-35	UK
-	45-50	UAE
-	35-40	UAE

Name	Age	Gender
Martin	23	M
Smith	32	F
Louis	19	M
Smith	32	F
Martin	23	M
Louis	19	M

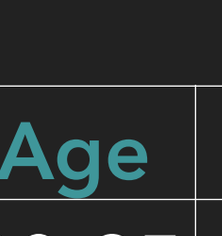
PRACTICE: WHAT TABLE IS K-ANONYMIZED?

Name	Age	Country
-	20-25	France
-	20-25	UK
-	30-35	France
-	30-35	UK
-	45-50	UAE
-	35-40	UAE

Name	Age	Gender
Martin	23	M
Smith	32	F
Louis	19	M
Smith	32	F
Martin	23	M
Louis	19	M

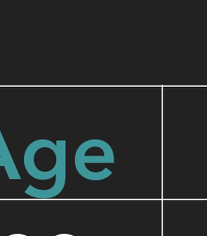
PRACTICE: WHAT TABLE IS K-ANONYMIZED?

Name	Age	Country
-	20-25	France
-	20-25	UK
-	30-35	France
-	30-35	UK
-	45-50	UAE
-	35-40	UAE



THIS TABLE IS NOT K-ANONYMISED (K=1). HOWEVER IT DOES NOT CONTAIN PERSONAL DATA, AS EACH ROW CANNOT IDENTIFY ONE SINGLE INDIVIDUAL

Name	Age	Gender
Martin	23	M
Smith	32	F
Louis	19	M
Smith	32	F
Martin	23	M
Louis	19	M



THIS TABLE IS K-ANONYMISED (K=2). IT DESCRIBES THE TREND OF ALL MARTIN'S TO BE 23 YEARS OLD MEN, REGARDLESS OF THE MEANINGFULNESS OF THIS INFORMATION

A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

PART. 3: SERVICES

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

DATA NEEDS TO BE KEPT
WITHDRAW CONSENT EASILY
EITHER UNLAWFUL, INACCURATE…

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

DATA IS NOT NECESSARY ANYMORE
DATA HAS BEEN UNLAWFULLY PROCESSED
THE DATA SUBJECT WITHDRAWS CONSENT

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

IF THERE IS ANY CHANGE IN THE DATA OR THE PROCESSING
(IF IT DOES NOT INVOLVES "DISPROPORTIONATE EFFORT")

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

INFORMATION TO PROVIDE:

GET

- IDENTITY AND CONTACT DETAILS OF THE CONTROLLER
- CONTACT DETAILS OF THE DPO
- PURPOSES OF THE PROCESSING
- LEGITIMATE INTERESTS OF THE CONTROLLER – IN SOME CASES
- PERIOD FOR WHICH THE DATA WILL BE STORED
- THE EXISTENCE OF THE RIGHTS OF THE DATA SUBJECT
- THE RIGHT TO LODGE A COMPLAIN WITH SUPERVISORY AUTHORITY
- THE MANDATORY NATURE OF THE DATA TO PROVIDE A SERVICE
- THE EXISTENCE OF AUTOMATED DECISION-MAKING

BE INFORMED

PO

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

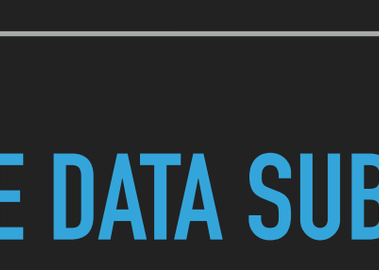
ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

ALL PERSONAL DATA CAN BE DOWNLOADED
IN A STRUCTURED, COMMONLY USED AND MACHINE-READABLE
FORMAT (CSV…)

ALL PERSONAL DATA CAN BE SENT DIRECTLY TO ANOTHER CONTROLLER



PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

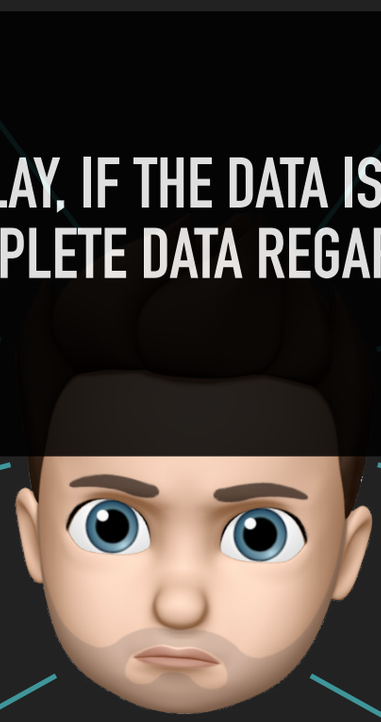
RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

WITHOUT DELAY, IF THE DATA IS INACCURATE
COMPLETION OF INCOMPLETE DATA REGARDING THE PROCESSING

GET NOTIFIED

BE INFORMED



PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

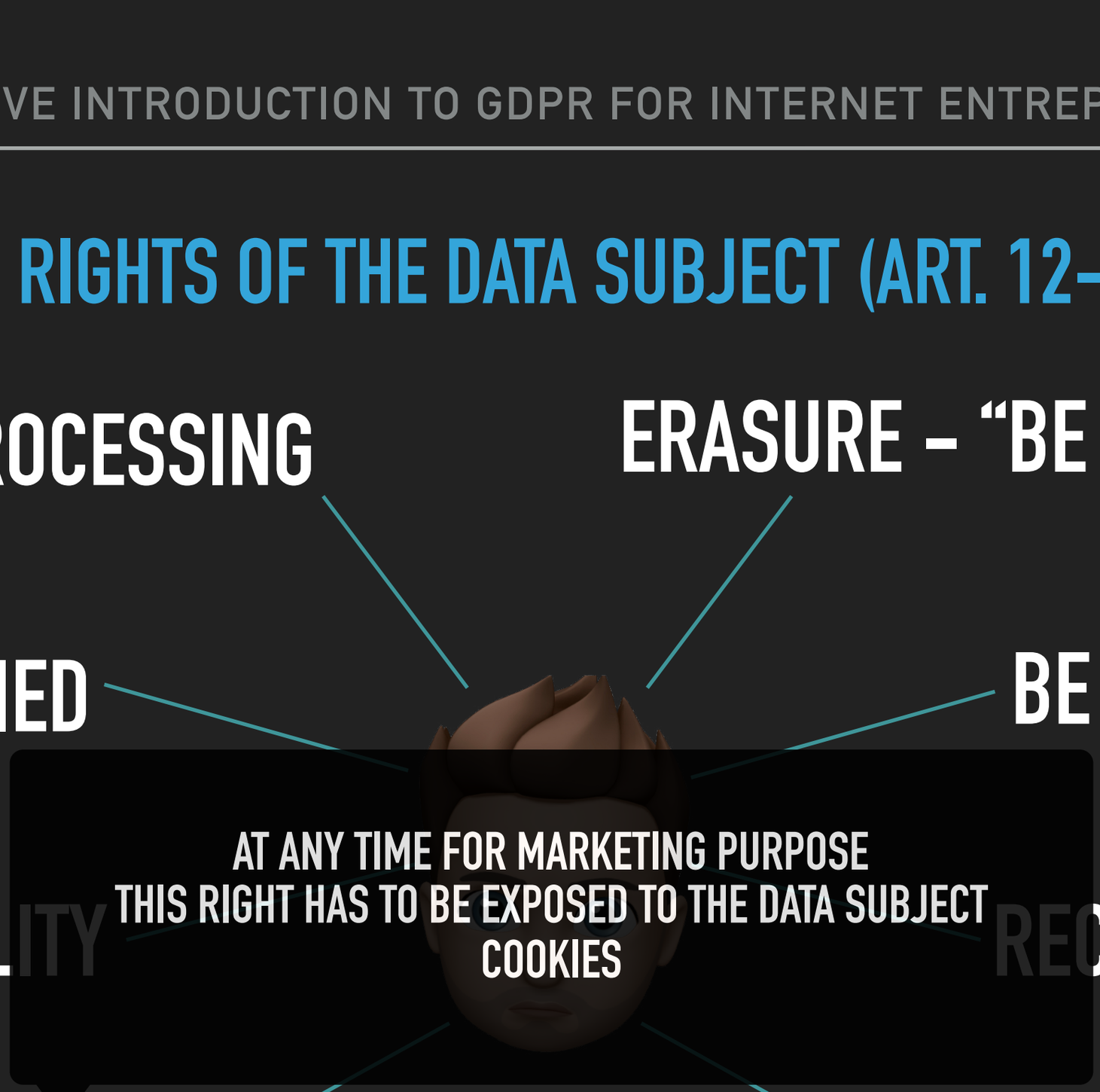
3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED



PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

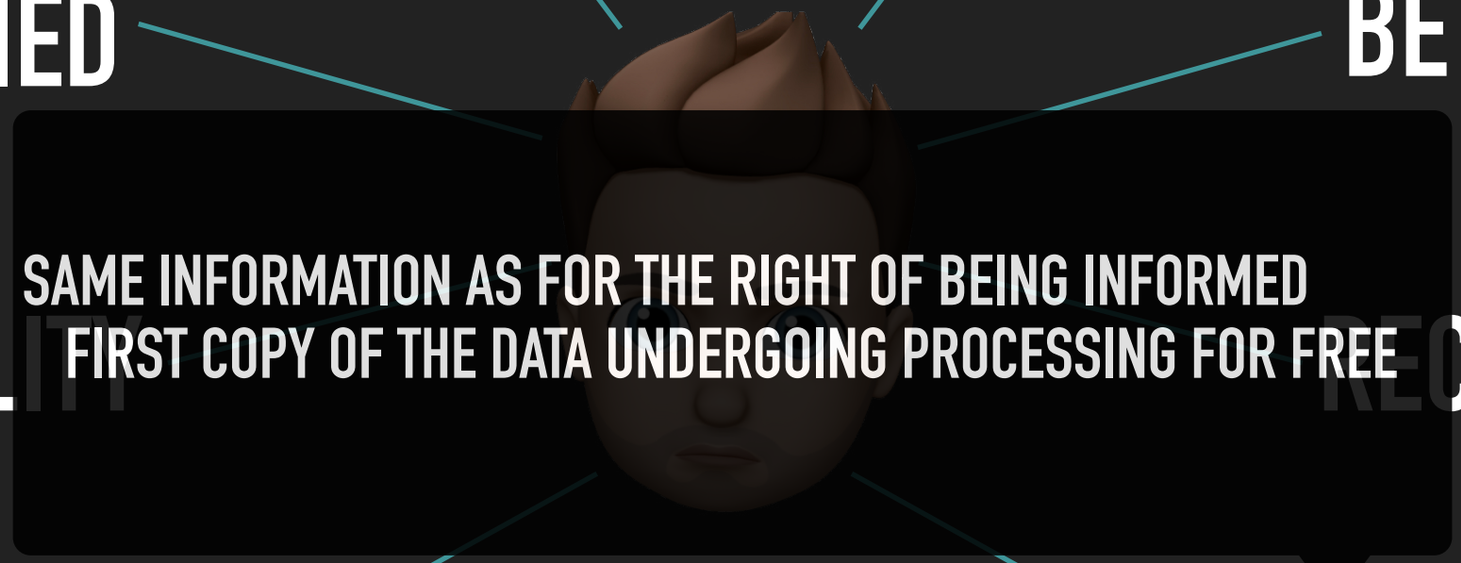
3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED



PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy
Registering form

PORTABILITY

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy
Registering form

PORTABILITY
Manually export from the databases
(At the beginning)

RECTIFY

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy
Registering form

PORTABILITY
Manually export from the databases
(At the beginning)

RECTIFY
Form to edit personal data

OBJECT

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy
Registering form

PORTABILITY
Manually export from the databases
(At the beginning)

RECTIFY
Form to edit personal data

OBJECT
Popup to accept/refuse the use of cookies

ACCESS

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy
Registering form

PORTABILITY
Manually export from the databases
(At the beginning)

RECTIFY
Form to edit personal data

OBJECT
Popup to accept/refuse the use of cookies

ACCESS
Contact form, DPO available

3. SERVICES: RIGHTS OF THE DATA SUBJECT (ART. 12–23)

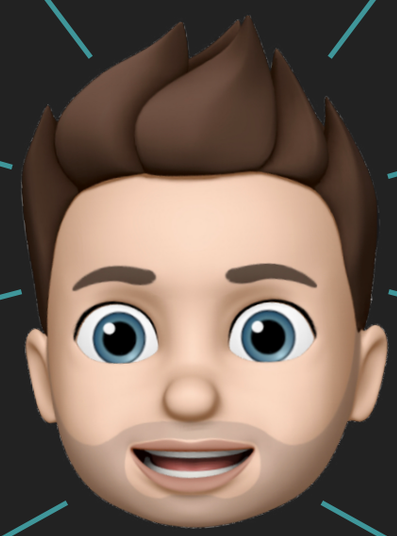
RESTRICT PROCESSING
Checkboxes to withdraw consent

ERASURE – "BE FORGOTTEN"
Add a button somewhere

GET NOTIFIED
Send emails on changes

BE INFORMED
Privacy policy

Registering form



PORTABILITY
Manually export from the databases

(At the beginning)

RECTIFY
Form to edit personal data

OBJECT
Popup to accept/refuse the use of cookies

ACCESS
Contact form, DPO available

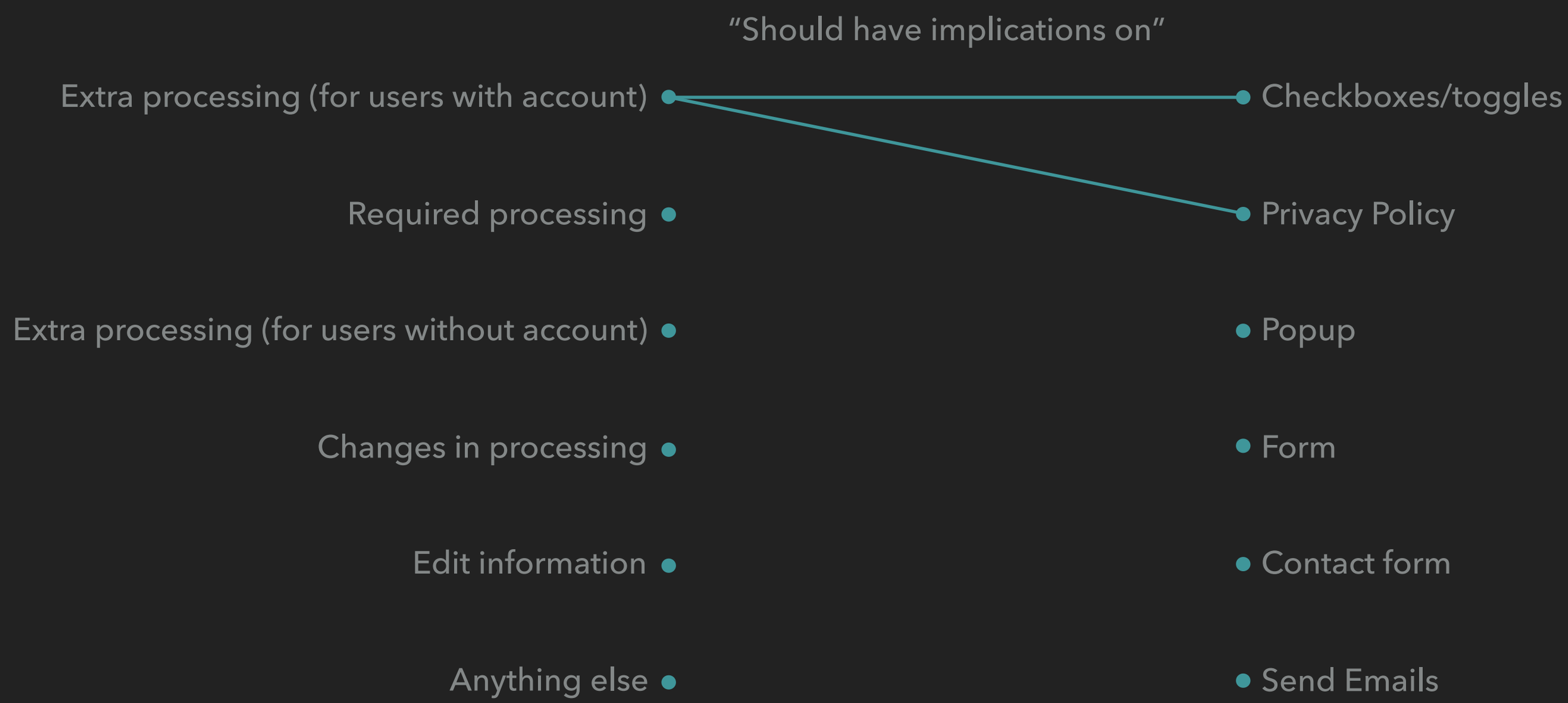
3. SERVICES: PRACTICE

"Should have implications on"

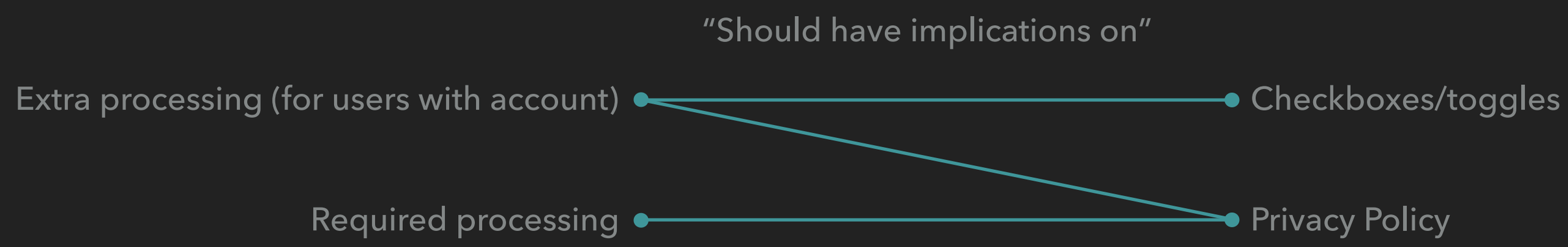
- Extra processing (for users with account)
- Required processing
- Extra processing (for users without account)
- Changes in processing
- Edit information
- Anything else

- Checkboxes/toggles
- Privacy Policy
- Popup
- Form
- Contact form
- Send Emails

3. SERVICES: PRACTICE



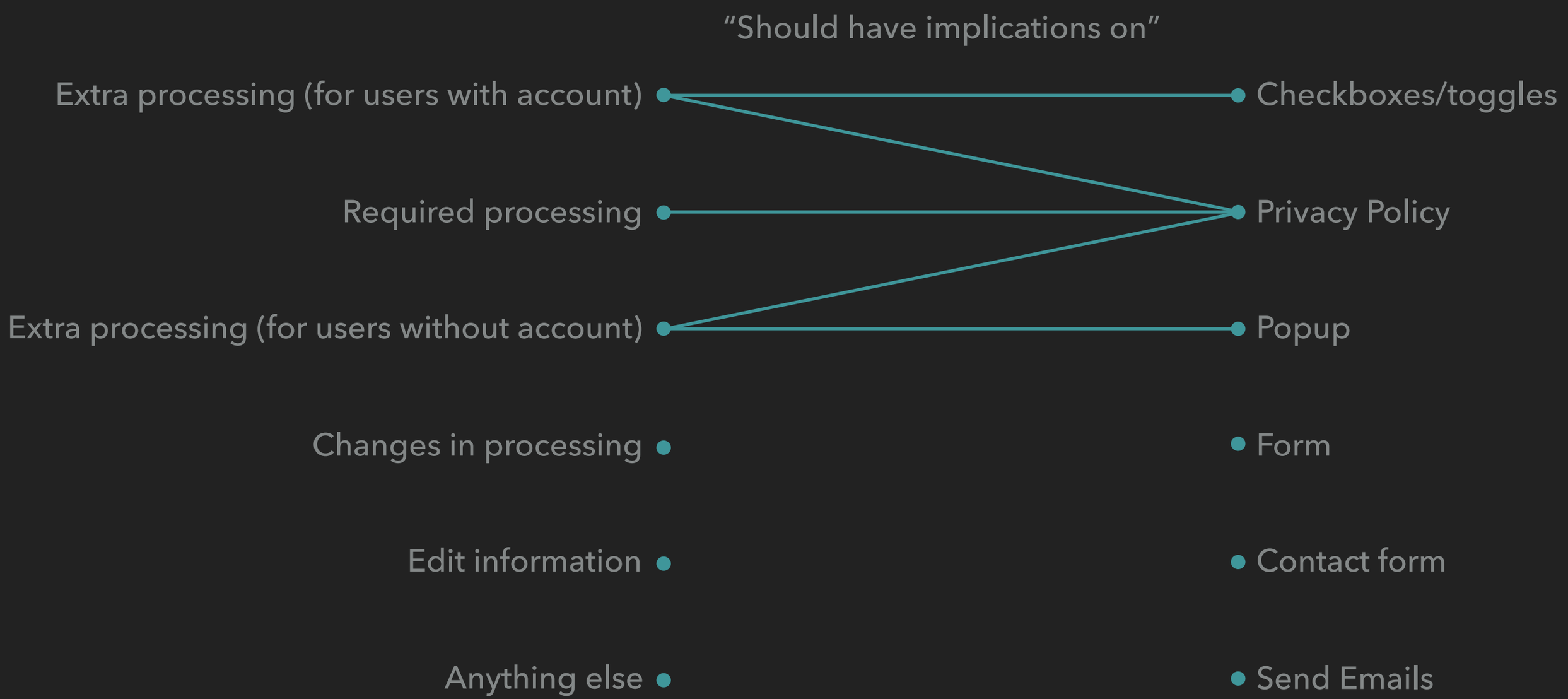
3. SERVICES: PRACTICE



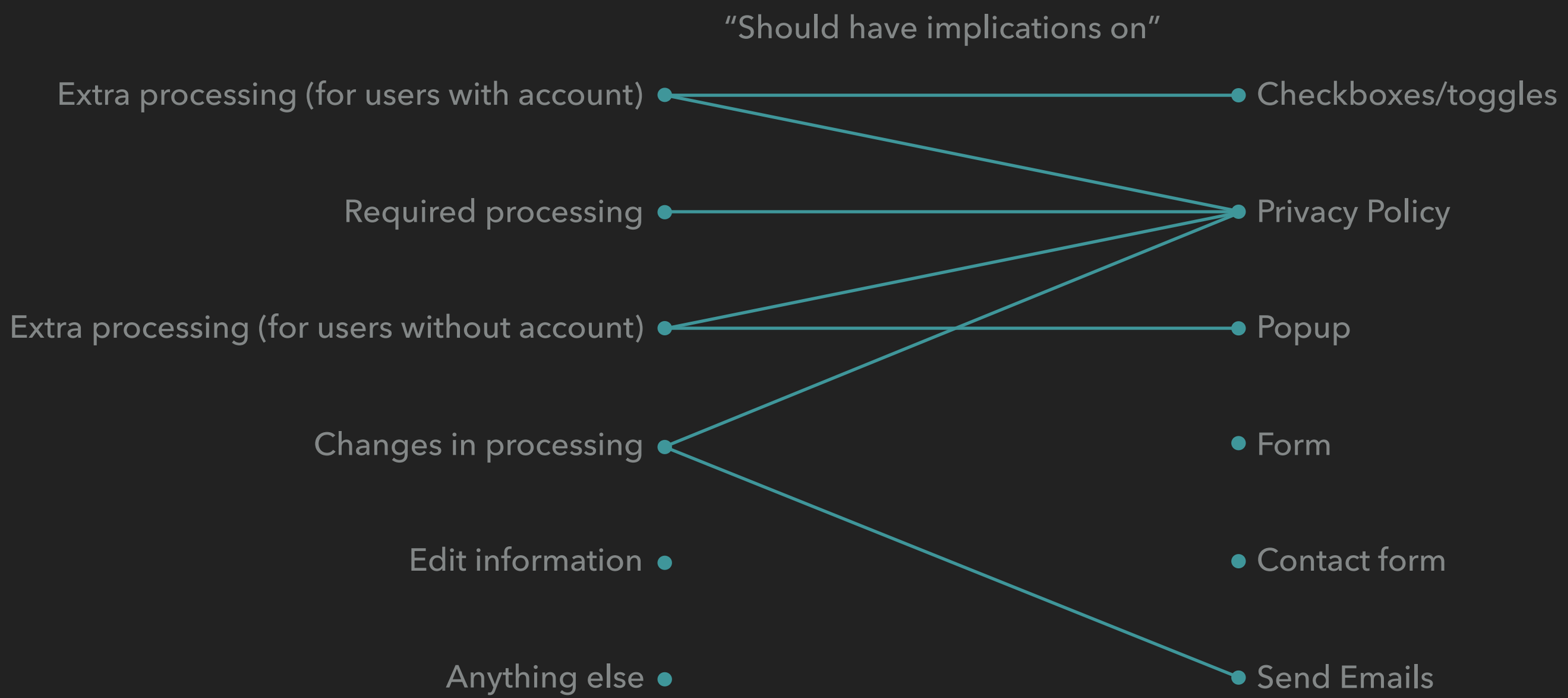
- Extra processing (for users without account)
- Changes in processing
- Edit information
- Anything else

- Popup
- Form
- Contact form
- Send Emails

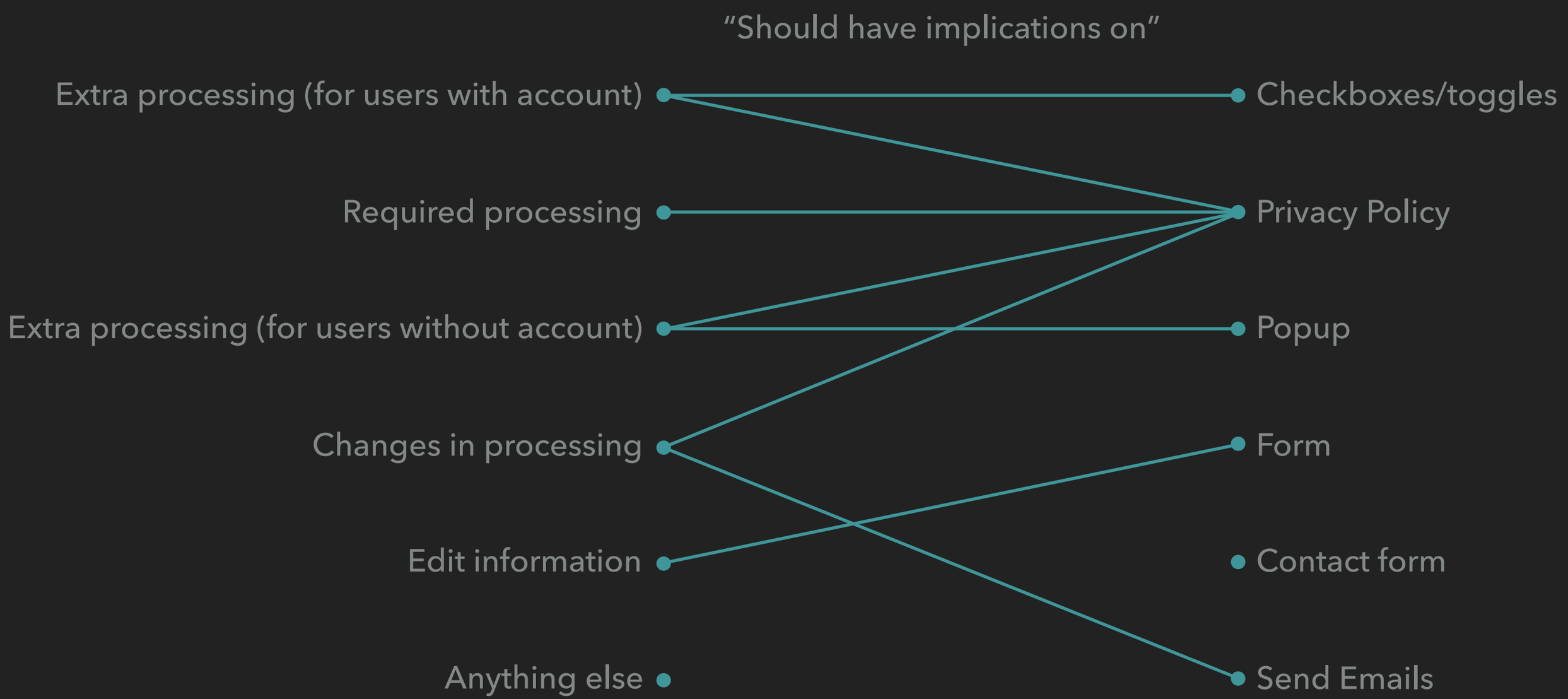
3. SERVICES: PRACTICE



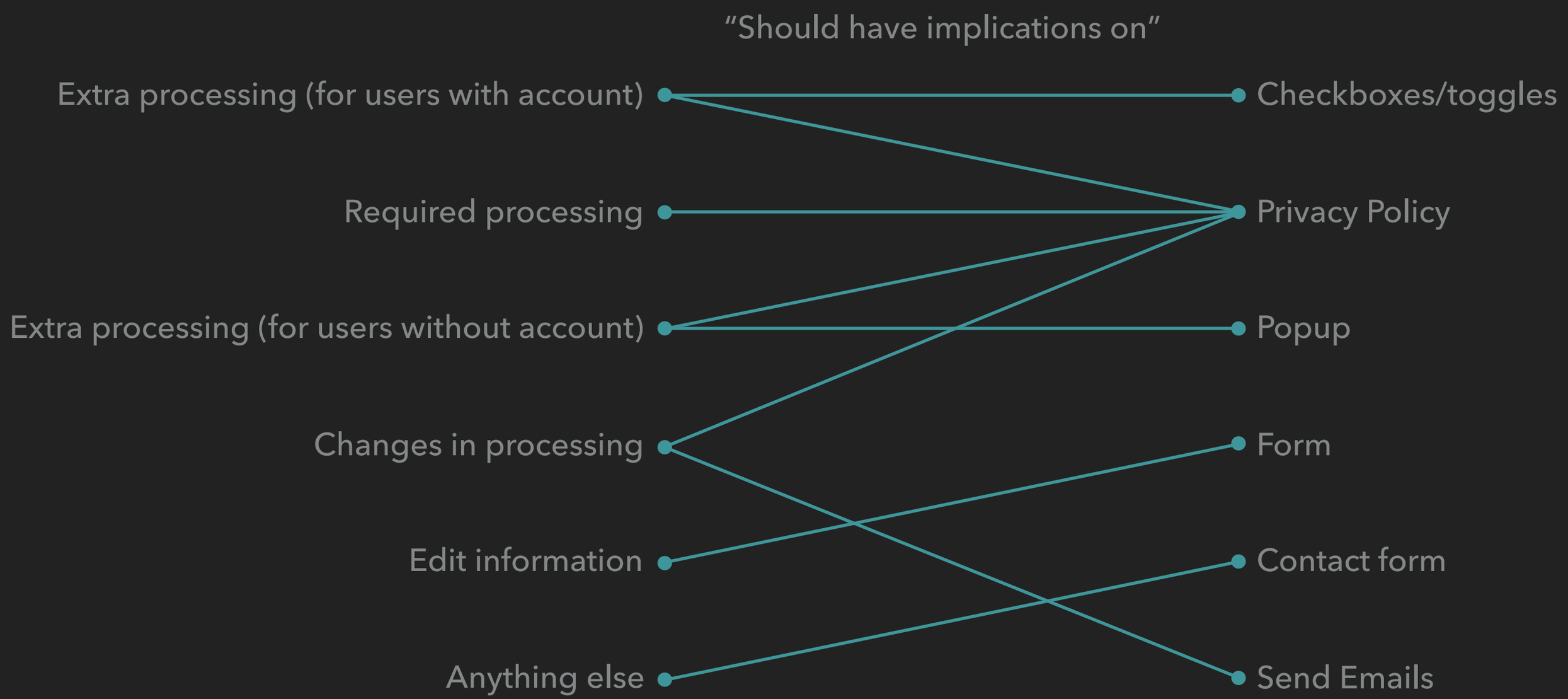
3. SERVICES: PRACTICE



3. SERVICES: PRACTICE



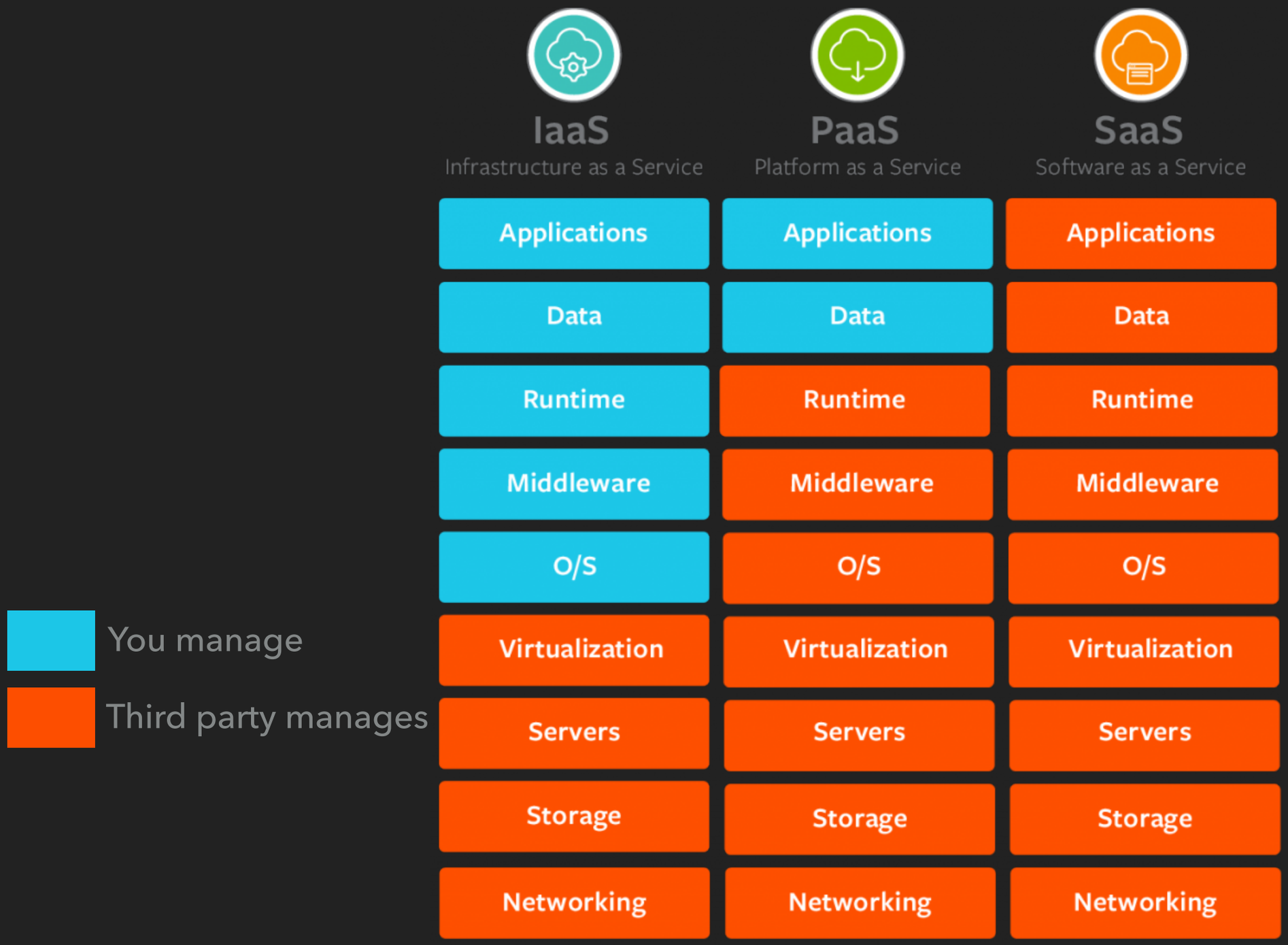
3. SERVICES: PRACTICE



A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

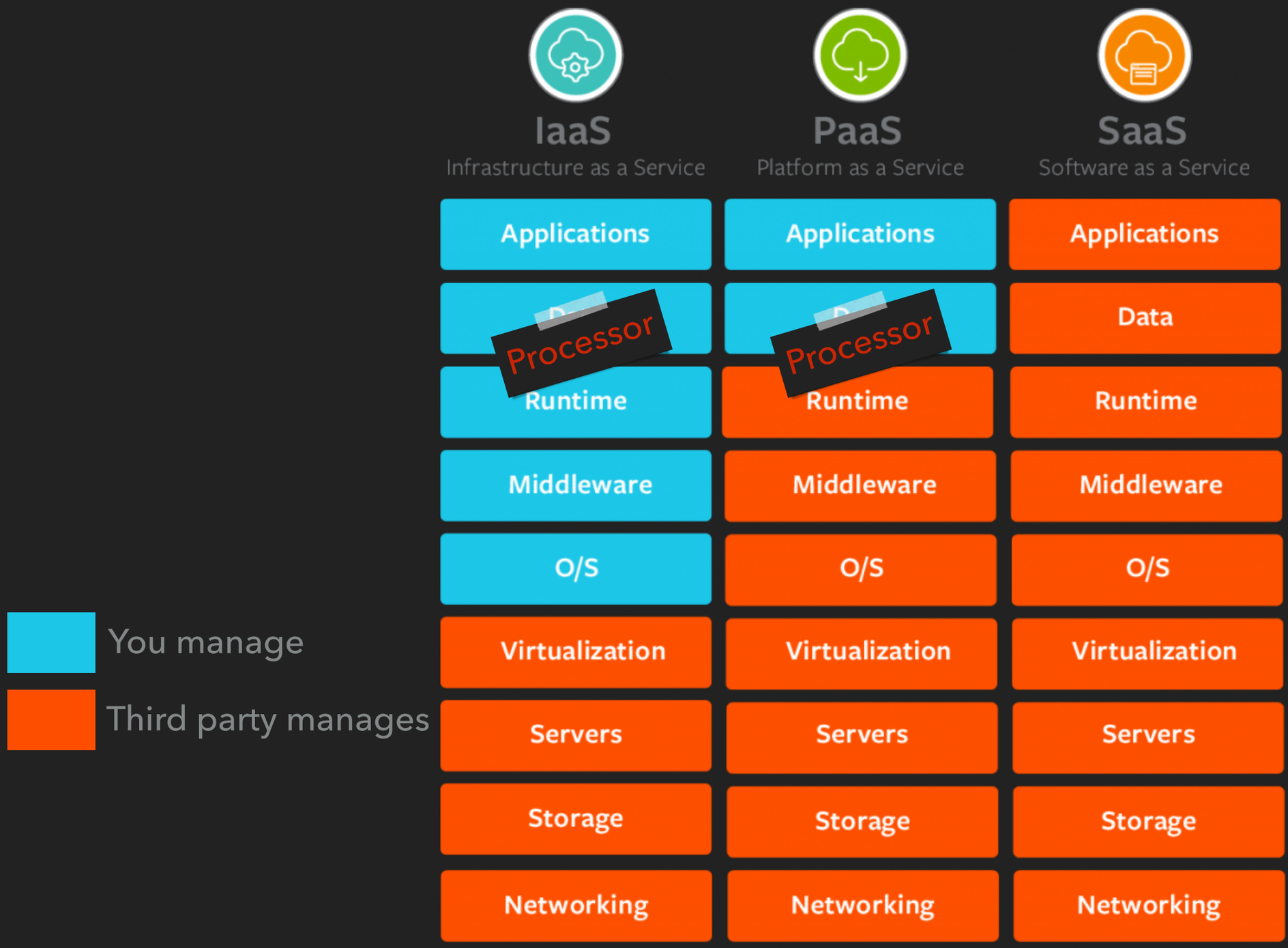
PART. 4: EXTERNAL SERVICES

4. EXTERNAL SERVICES: HOSTING – IAAS, PAAS, SAAS



Source: www.bmc.com

4. EXTERNAL SERVICES: HOSTING – IAAS, PAAS, SAAS

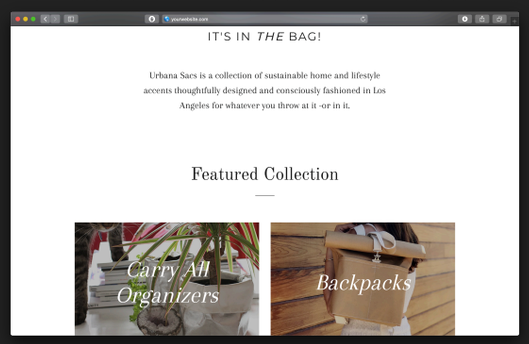


Source: www.bmc.com

4. EXTERNAL SERVICES: CATEGORIES OF SAAS

- All-included ready-to-use services (Shopify)
- Backend as a service (Firebase, Authentification, Analytics…)
- Add-on services (Payment, Captcha, Messaging, ChatBot, Search bar…) - front+back
- Internal tool as a service (AirTable, ~~Back Office~~…)

4. EXTERNAL SERVICES: ALL-INCLUDED



You (your website)

Services

Data

Shopify

Services

Data

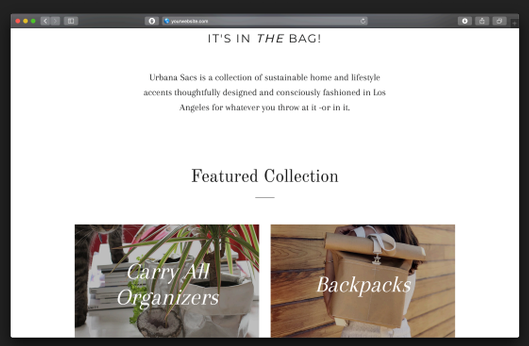
Services

Data

Your user

GDPR | Data | Services | External Services

4. EXTERNAL SERVICES: ALL-INCLUDED



You (your website)

Services

Data

Controller

Shopify

Services

Data

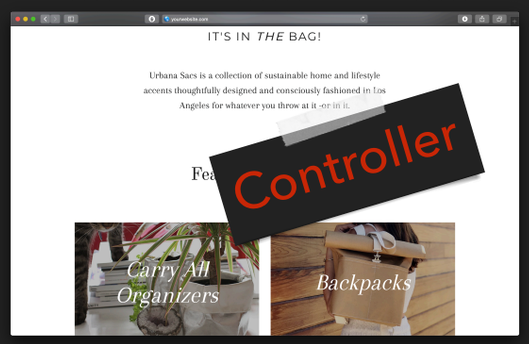
Services

Data

Your user

GDPR | Data | Services | External Services

4. EXTERNAL SERVICES: ALL-INCLUDED



You (your website)

Services

Data

Shopify

Services

Data

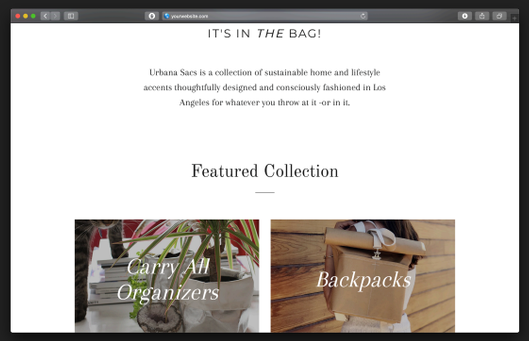
Services

Data

Your user

GDPR | Data | Services | External Services

4. EXTERNAL SERVICES: BACKEND AS A SERVICE & ADD-ONS



You (your website)

Services (Administration…)

Data

Firebase

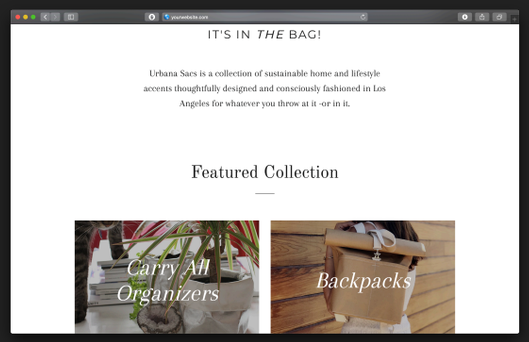
Services

Data

Your user

GDPR | Data | Services | External Services

4. EXTERNAL SERVICES: BACKEND AS A SERVICE & ADD-ONS



You (your website)

Services (Administration…)

Data

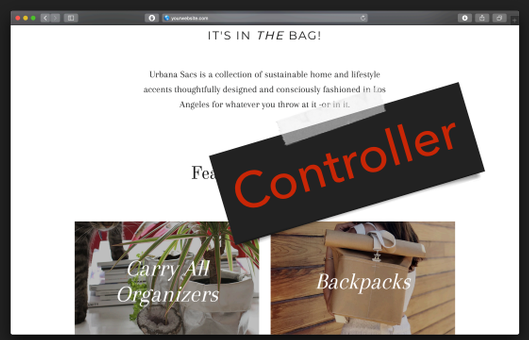
Firebase

Services

Data

Your user

4. EXTERNAL SERVICES: BACKEND AS A SERVICE & ADD-ONS



You (your website)

Services (Administration…)

Data

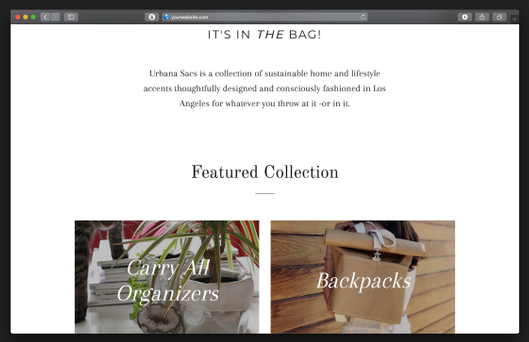
Firebase

Services

Data

Your user

4. EXTERNAL SERVICES: INTERNAL TOOLS AS A SERVICE



You (your website)

Services

Data

Airtable

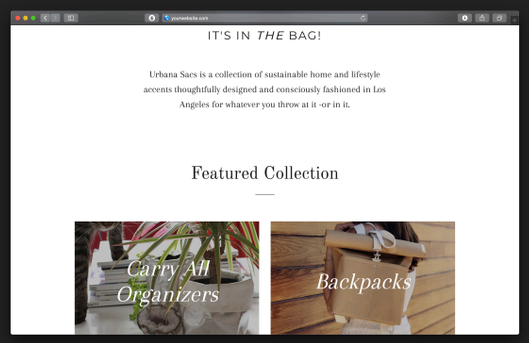
Services

Data

Your user

GDPR | Data | Services | External Services

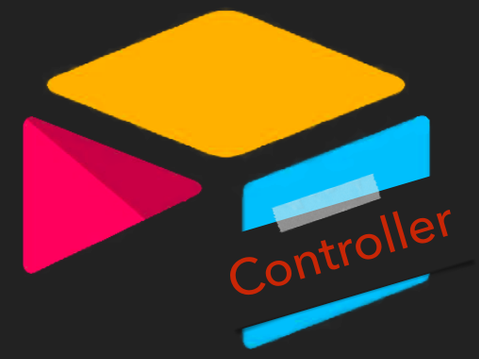
4. EXTERNAL SERVICES: INTERNAL TOOLS AS A SERVICE



You (your website)

Services

Data



Airtable

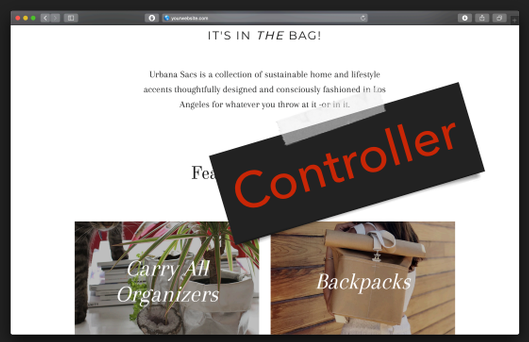
Services

Data

Your user

GDPR | Data | Services | External Services

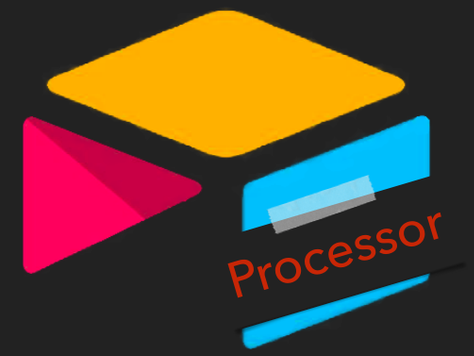
4. EXTERNAL SERVICES: INTERNAL TOOLS AS A SERVICE



You (your website)

Services

Data



Airtable

Services

Data

Your user

GDPR | Data | Services | External Services

4. EXTERNAL SERVICES: BREACH FROM THE PROCESSOR

- The processor informs you “instantly”
- You (controller) have 72 hours to tell a supervisory authority
- Massive leaks of commonly used processor have not happened

Thank you for your attention!

A COMPREHENSIVE INTRODUCTION TO GDPR FOR INTERNET ENTREPRENEURS

PRACTICE

PRACTICE: TRAVEL OPTIMIZER APPLICATION – SCENARIO

- The user inputs all the places he/she wants to go to (location, minimum time to stay)
- The application proposes an optimization of all the trips, including places to stay (plane, train, car rental, hotel…)
- The “community” page of the app displays distances traveled by other users
- Analytics about the preferred way of transportation (location, age, way of transportation)
- Total distance traveled by all the users combined ever

PRACTICE: TRAVEL OPTIMIZER APPLICATION

First Name

Email address

Credit Card Number

Last Name

Transportation cards/Royalty plans

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

Home Address

Passport number

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT QUESTION SHOULD YOU ASK YOURSELF?

First Name

Email address

Credit Card Number

Last Name

Transportation cards/Royalty plans

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

Home Address

Passport number

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT QUESTION SHOULD YOU ASK YOURSELF?

First Name

Last Name

Email address

Transportation cards/Royalty plans

Credit Card Number

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

Home Address

Passport number

ANSWER: IS IT PERSONAL DATA? IS IT NEEDED TO PROVIDE THE SERVICES?

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT DATA DO YOU KEEP?

First Name

Email address

Credit Card Number

Last Name

Transportation cards/Royalty plans

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

Home Address

Passport number

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT DATA DO YOU KEEP?

First Name

Email address

~~Credit Card Number~~

Last Name

Transportation cards/Royalty plans

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

~~Home Address~~

~~Passport number~~

Ask for the starting place, store it locally

ANSWER

PRACTICE: TRAVEL OPTIMIZER APPLICATION

EXTERNAL SERVICES: WHAT TO CHECK?

Get booking data	Google Maps Platform API
	booking.com API
	AirBnB API
	Google Flight API
Contacting the DPO	Intercom
Authentification	auth0
Display analytics	AirTable

Privacy Policy

Terms of Use

PRACTICE: TRAVEL OPTIMIZER APPLICATION

EXTERNAL SERVICES: WHAT TO CHECK?

Get booking data	Google Maps Platform API	Nothing (no personal data involved)
	booking.com API	Nothing (no personal data involved)
	AirBnB API	Nothing (no personal data involved)
	Google Flight API	Nothing (no personal data involved)
Contacting the DPO	Intercom	Privacy Policy AND Terms of use (personal data of your employees AND users)
Authentification	auth0	Terms of use (personal data of your users)
Display analytics	AirTable	Terms of use (data is not supposed to be personal)

ANSWER

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT MICRO SERVICES (APIS) WILL BE USED?

First Name

Email address

Credit Card Number

Last Name

Transportation cards/Royalty plans

Age

Calendar events

Car - cost per kilometer

For each place to go to
-Location
-Minimum stay

Home Address

Passport number

Intercom

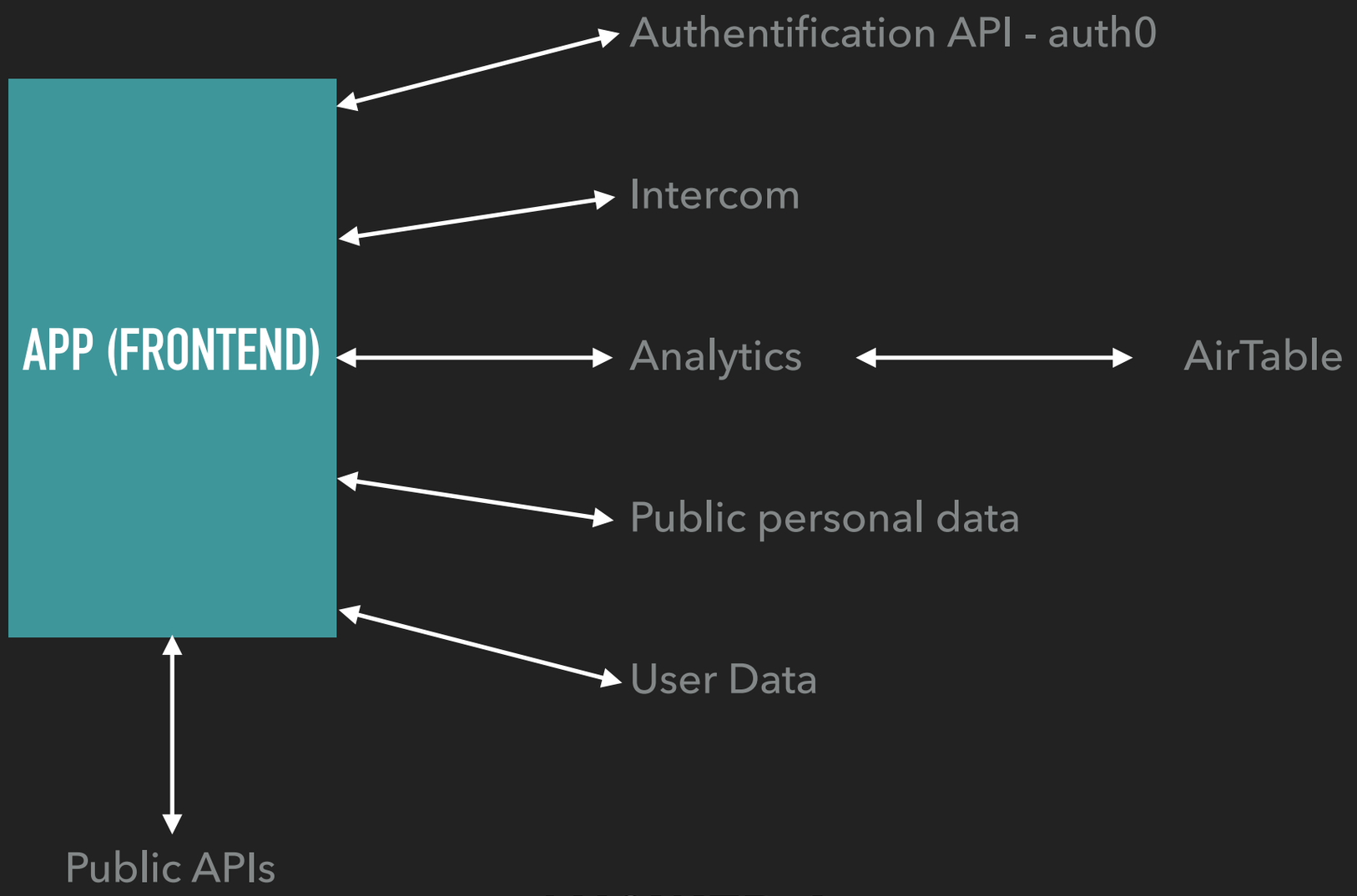
auth0

AirTable

Public APIs

PRACTICE: TRAVEL OPTIMIZER APPLICATION

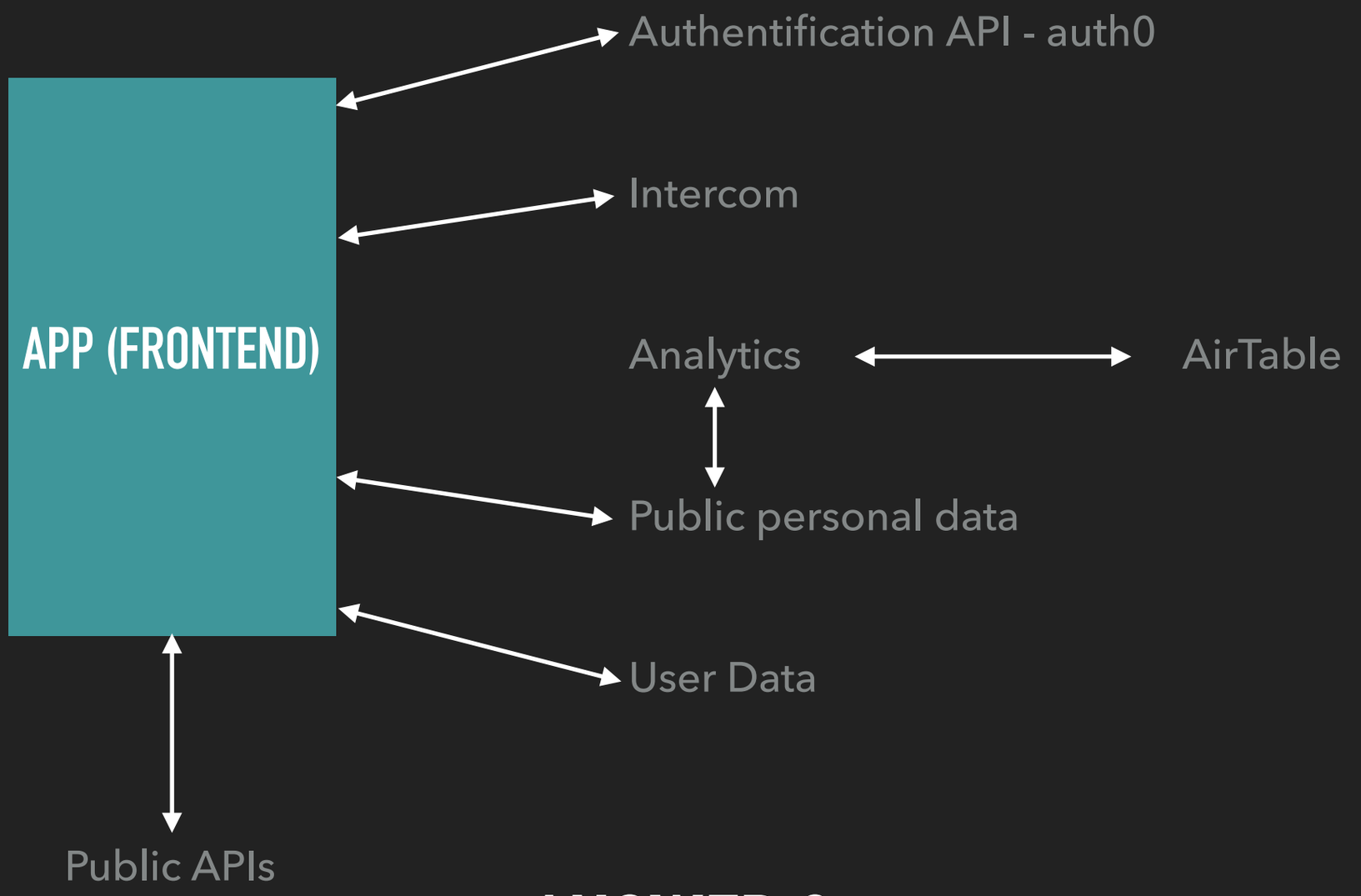
WHAT MICRO SERVICES (APIS) WILL BE USED?



ANSWER 1

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT MICRO SERVICES (APIS) WILL BE USED?



ANSWER 2

PRACTICE: TRAVEL OPTIMIZER APPLICATION

WHAT MICRO SERVICES (APIS) WILL BE USED?

Authentification API - auth0	POST auth information, return auth token
Intercom	
Analytics	Do not store any data. Only translate and post on AirTable (anonymized data)
User Data	SQL+noSQL, sample data for debugging, store consent, pseudonymise if possible
Public personal data	noSQL
Public APIs	No personal data involved

ANSWER – ROLE OF EACH SERVICE

DONE

THANK YOU!

QUESTIONS?