

Rights of the Data Subjects and Lawful Processing of Personal Data

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

General Data Privacy Principles

transparency

explicitability
clarity
simplicity
perceptibility
unambiguity
manifestness
decipherability
translucence
openness
conspicuousness
cleanness



General Data Privacy Principles

legitimate purpose

lawful objective reasonable justifiable authorized sanctioned

genuine appropriate statutory proper accepted

fair

PROPERTY OF

General Data Privacy Principles

proportionality

reciprocal
equitable
commensurate
even
rational
correlative
corresponding
comparable
equal
just
comparative

PROPERTY C

Transparency: Rights of the Data Subject

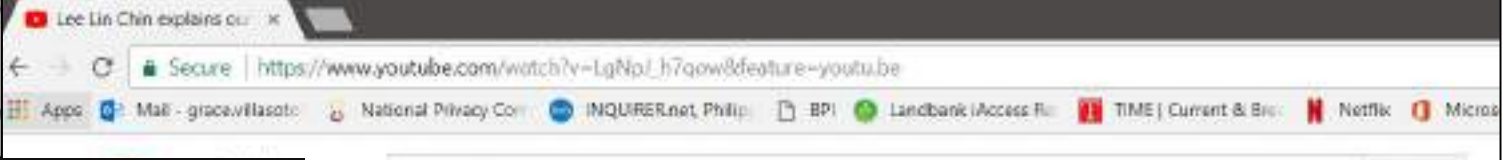
Right to INFORMATION

WHAT INFORMATION MUST BE SUPPLIED?	WHEN SHOULD INFORMATION BE PROVIDED?
1. Description of the personal data	<ul style="list-style-type: none">• before the entry of personal data into the processing systemor• at the next practical opportunity
2. Purposes for processing; including: direct marketing, profiling, or historical, statistical or scientific purpose	
3. Basis of processing (legal mandate, contract, etc.)	
4. Scope and method of the processing	
5. Recipients/classes of recipients to whom the personal data are or may be disclosed	
6. Identity and contact details of the personal information controller	
7. Retention period	
8. Existence of rights as data subjects.	

NPC's Privacy Notice

Personal Information

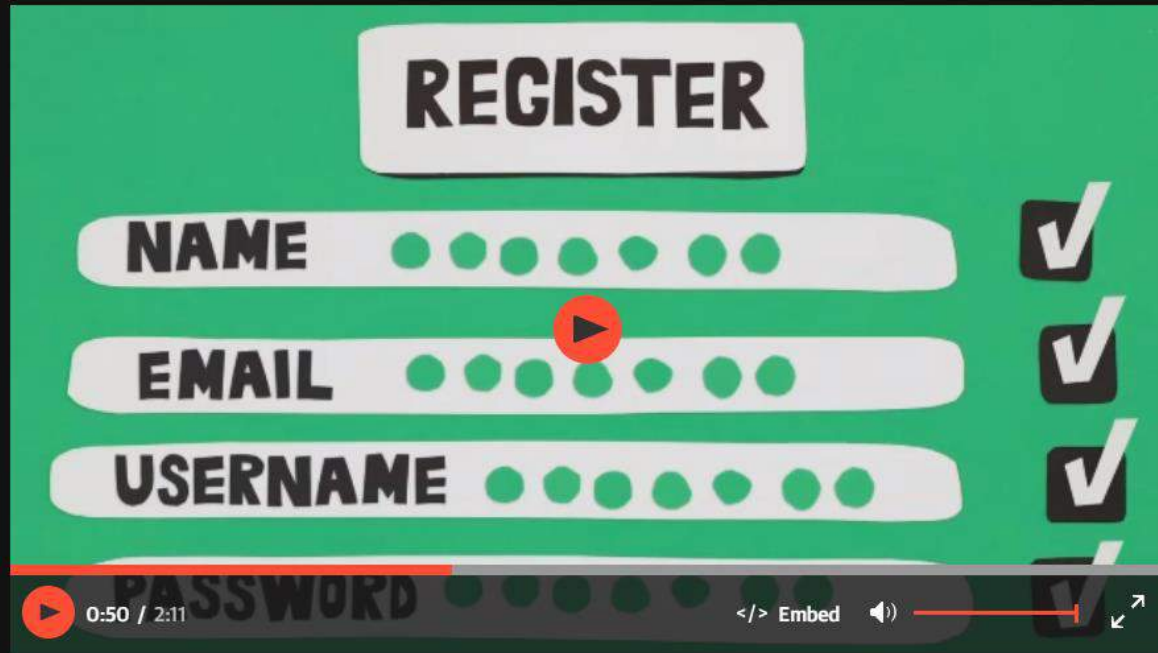
We collect the following personal information



Lee Lin Chin explains our...
Secure | https://www.youtube.com/watch?v=LgNpL_h7qow&feature=youtu.be
Apps Mail - grace.willasoto National Privacy Comm INQUIRER.net, Philip BPI Landbank (Access R TIME | Current & Bic Netflix Micros

Search

Our privacy policy - a quick look



REGISTER

NAME [dots] ✓

EMAIL [dots] ✓

USERNAME [dots] ✓

PASSWORD [dots] ✓

0:50 / 2:11 Embed

An animation of some of the key points from the Guardian's privacy policy. What types of data do we collect from you? What do we use it for? And how can you contact us if you have any questions?



WHY SHOULD I TRUST YOU WITH MY PERSONAL DATA?

1:14 / 3:13

Lee Lin Chin explains our deal with your data

For any questions, queries or complaints, please contact the DPO:
Skyland Plaza Sen. Gil Puyat Avenue Cor. Tindalo Street, Makati City
Telephone No. (632) 5119815
dpo-gi@assa.com.ph

Transparency: Rights of the Data Subject

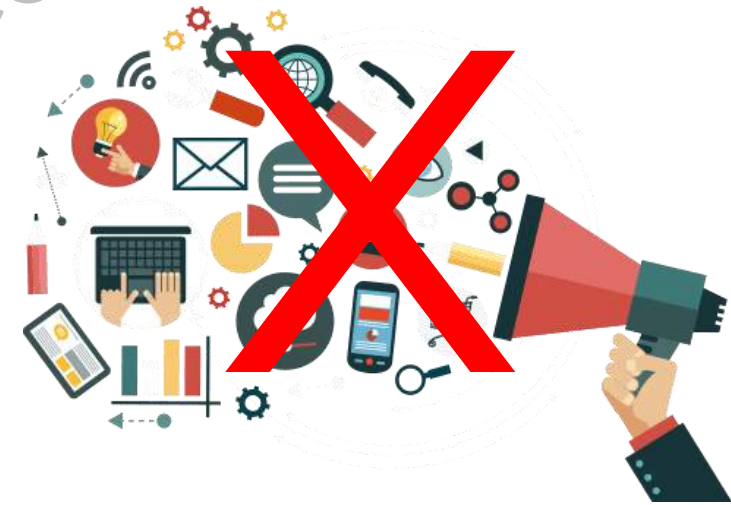
Right to OBJECT

When does the right to object apply?

- processing is based on consent (includes direct marketing)
- processing is based on legitimate interest

If processing is for direct marketing purposes:

- PIC must stop processing upon receipt of data subject's objection.

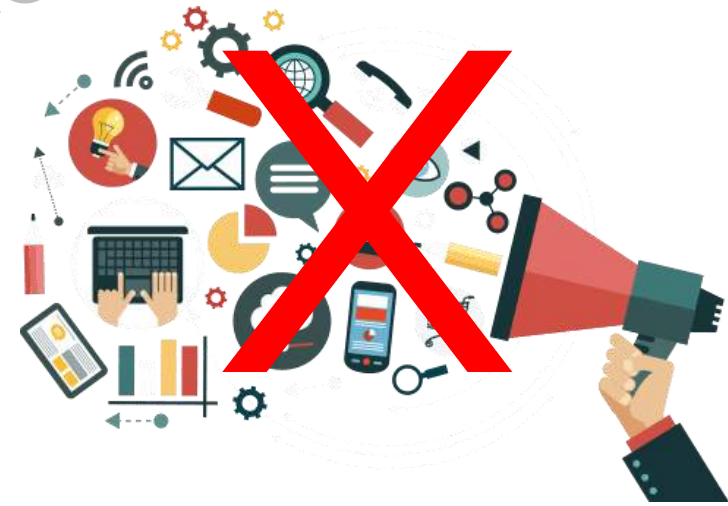


Transparency: Rights of the Data Subject

Right to OBJECT

When a data subject objects/withholds consent, the PIC shall no longer process the personal data, unless the processing is:

1. Pursuant to a subpoena;
2. For obvious purposes, i.e. contract, employer-employee relationship, etc.; or
3. Result of a legal obligation.



Transparency: Rights of the Data Subject

Right to ACCESS

Reasonable access to the following:

1. Contents of personal data;
2. Sources of personal data;
3. Names & addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data, if any;
6. Information on automated processes: where the data will or likely to be made as the sole basis for any decision that significantly affects the data subject;
7. Date when his or her personal data concerning the data subject were last accessed/modified; and
8. Name and address of the PIC.

Transparency: Rights of the Data Subject

Right to ERASURE OR BLOCKING



When does the right apply?

- a. When personal data is:
 - incomplete, outdated, false, or unlawfully obtained
 - used for unauthorized purpose
 - no longer necessary for the purpose
- b. Data subject withdraws consent/objects to the processing, and there is no other legal ground/legitimate interest for processing.
- c. Processing is unlawful.
- d. PIC or PIP violated the rights of the data subject.

Transparency: Rights of the Data Subject

Right to RECTIFICATION

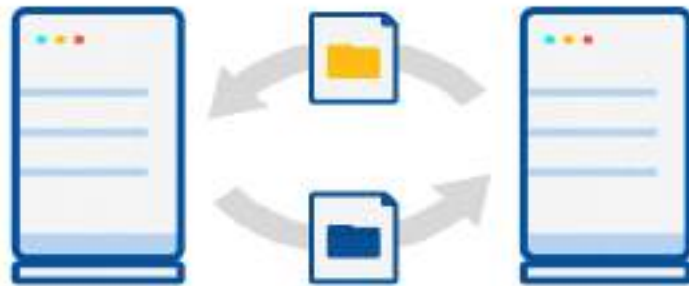
- Right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately, unless the request is vexatious or otherwise unreasonable.
- If personal data was disclosed to third parties: PIC must inform them of the rectification upon reasonable request of the data subject.



Transparency: Rights of the Data Subject

Right to DATA PORTABILITY

- Right to obtain from the PIC a copy of personal data in an electronic/ structured format that is commonly used/allows further use by the data subject.
- What are the conditions for this right to apply?
 - ✓ personal data requested concerns the data subject making the request;
 - ✓ personal data is processed electronically; and
 - ✓ processing is based on consent or contract



Transparency: Rights of the Data Subject

Right to DAMAGES

The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

See: NPC Circular No. 16-04 – Rules of Procedure

Transparency: Rights of the Data Subject


Right to DAMAGES



CNN Health » Diet + Fitness | Living Well | Parenting + Family | Vital Signs International Edition +

Aetna customers get \$17 million in HIV privacy settlement

By Jacqueline Howard, CNN
Updated 1734 GMT (0134 HKT) January 17, 2018



"This is ... the largest data breach involving HIV-related privacy," lawyer says

The lawsuit was filed in August after some 12,000 Aetna customers nationwide received letters mailed in July that accidentally revealed their HIV status through the windows of the envelopes, indicating they were taking either HIV medications or PrEP, a pre-exposure prophylactic that prevents HIV.

Under the terms of the proposed settlement, which is now subject to court approval, Aetna has agreed to pay \$17,161,200 to resolve the privacy breach claims.



Consent

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

Legitimate Purpose: Consent



- The data subject agrees to the collection and processing of personal information
 - ✓ **Freely given**
 - ✓ **Specific**
 - ✓ **Informed indication of will**
- Evidenced by written, electronic or recorded means:
 - ✓ signature
 - ✓ opt-in box/clicking an icon
 - ✓ sending a confirmation email
 - ✓ oral confirmation
- **Opt-in:** silence, pre-ticked boxes or inactivity does not constitute consent

Freely given, specific, and informed

- Consent means giving data subjects **genuine choice and control** over how a PIC uses their data.
- Data subjects must be able to refuse consent, and must be able to withdraw consent easily at any time.
- Consent should be **unbundled from other terms and conditions** (including giving **granular consent options** for different types of processing) wherever possible.
- Clear affirmative action means someone must take deliberate action to opt in.

Unbundled Consent

Terms & Conditions

Terms and conditions – website usage

Welcome to the DPN website. The Data Protection Network (DPN) is a trading name for Opt-4 Ltd. If you continue to browse and use this website, you are agreeing to comply with the following terms and conditions of use, which together with our [privacy policy](#), govern DPN's dealings with you in relation to this website. If you disagree with any part of these terms and conditions, please do not use our website.

DPN may amend these Terms and Conditions at any time by posting the amended Terms and Conditions on the DPN site.

The term DPN or 'us' or 'we' refers to the owner of the website whose registered office is at Boundary House, Boston Road, London W7 2QE, UK. The term 'you' refers to the user or viewer of our website or to those who become members of DPN.

The use of this website is subject to the following terms of use:

- The content of the pages of this website is for your general information and use only. It is subject to change without notice.
- The information provided and the opinions expressed in this website represent the views of the authors and contributors. They do not constitute legal advice and cannot

I agree to the Terms & Conditions

Join our mailing list.

Data Protection Network

Submit and Confirm »

Granular Consent

Dairy, Eggs & Fridge	Pantry	Freezer	Drinks	Liquor	Tobacco	Pet	Baby
<p>Communication preferences</p> <p>Yes! I would like to receive updates about products & services, promotions, special offers, news & events from Woolworths Online via</p> <p> <input type="checkbox"/> SMS <input type="checkbox"/> Email </p> <p><input checked="" type="checkbox"/> Samples - Yes I would like to receive FREE Samples from time to time.</p>							
Privacy	T&Cs	Collection Notice	Business Orders	<input type="button" value="Sign up >"/>			

PROPER

I have read and agreed to the terms and conditions stated above.

We may contact you about products and services you may like unless you click to opt out.

I'd like to receive exclusive discounts and updates from XYZ by email, post and SMS.

Please untick this box if you would not like to receive emails from XYZ on offers and news.

This consent form is confusing as the first tickbox asks for positive action to **signify agreement**, while the second asks for a positive action to **signify refusal**.

A consent form like this has issues because it uses pre-ticked boxes and mixes them with unticked ones.

Is consent always needed?

- No. Consent is just one criterion for lawful processing of both personal and sensitive personal information.
- Consent will not always be the most appropriate basis for processing personal data.
- PICs should choose the lawful basis that most closely reflects the true nature of the relationship with the individual and the purpose of the processing.

Processing which may not need consent:



**Securities and
Exchange
Commission**
PHILIPPINES



PROPERTY C

What are the alternatives to consent?

For processing of personal information:

- **Contract with the individual:** to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.
- **Compliance with a legal obligation:** if you are required by law to process the data for a particular purpose.
- **Vital interests:** you can process personal information if it is necessary to protect the data subject's life and health.
- **National emergency:** to respond to national emergency or to comply with the requirements of public order and safety.
- **Public task:** if you need to process personal information to carry out public function or service and you have a legal basis for the processing.
- **Legitimate interests:** for the private sector, you can process personal data without consent if you have a genuine and legitimate reason, unless this is overridden by fundamental rights and freedoms of the data subject.

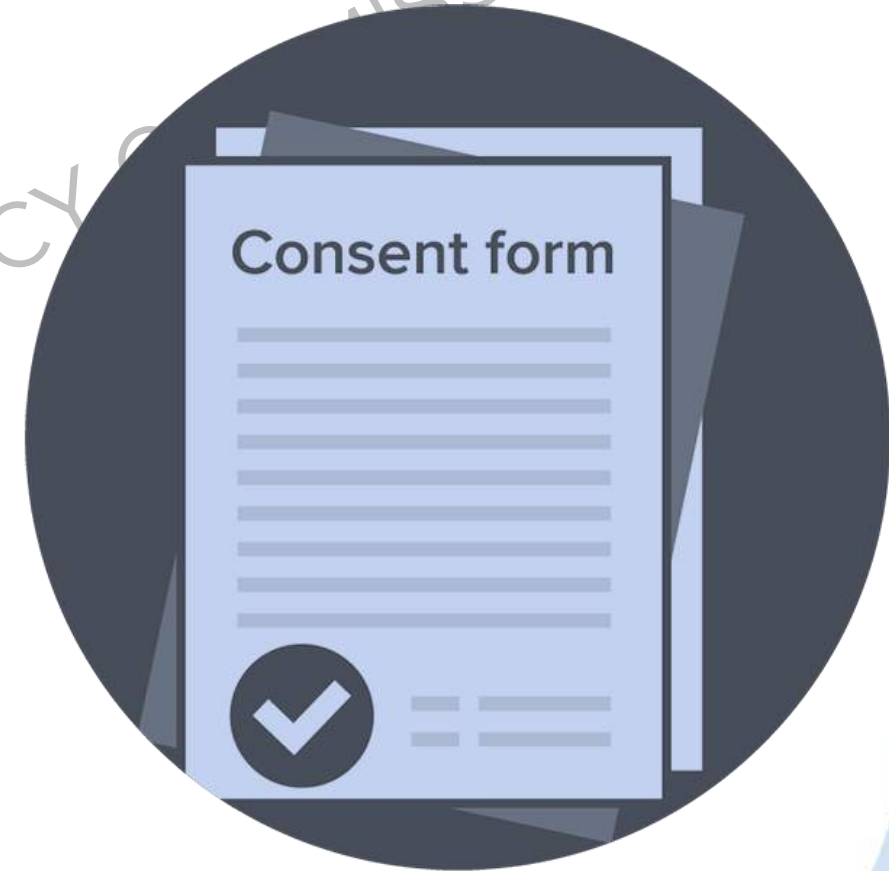
What are the alternatives to consent?

For processing of sensitive personal information:

- **Existing law and regulation:** you can process sensitive personal information (SPI) when there is a regulatory enactment which requires the processing of such data
- **Protection of life and health:** to protect someone's life – the data subject or another person, and the data subject is not legally/physically able to express his consent
- **Public organizations:** this refers to processing done by non-stock, non-profit organizations, cooperatives, and the like, where processing is only confined and related to the bona fide members of these organizations or their associations
- **Medical treatment:** when processing is carried out by a by a medical practitioner or a medical treatment institution, and there is adequate level of protection of SPI
- **Lawful rights and interests:** when processing is necessary to protect lawful rights and interests of in court proceedings, in the establishment/exercise/defense of legal claims, or when provided to government or public authority.

Consent: Next Steps

1. Identify all processing activities which are legitimized through data subjects' consent.
2. Evaluate whether you may rely on existing consent in the identified activities or whether other processing criteria/basis can be relied on in certain instances.
3. Where consent is relied on:
 - a. check whether it is:
 - freely given;
 - specific;
 - informed; and
 - evidenced by written, electronic or recorded means



Consent: Next Steps

- b. vet and amend existing consent forms to ensure they are in line with formal requirements.
4. Ensure processes are in place to promptly honor any withdrawals of consent (including that affected processing operations are stopped).
5. Put in place systems creating reliable records of consents which will enable organizations to demonstrate compliance with consent requirements.



Legitimate Interest

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

What is the “legitimate interests” criterion?

- Section 12(f) - The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution
- Calls for a balancing test: the legitimate interests of the PIC (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject.

What is the “legitimate interests” criterion?

- An interest can be considered as legitimate as long as the PIC can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be ‘acceptable under the law’.
- A 'legitimate interest' must therefore:
 - be lawful (i.e. in accordance with applicable law);
 - be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
 - represent a real and present interest (i.e. not be speculative)

Scenario 1 - special offer by a pizza chain

Claudia orders a pizza via a mobile app on her smartphone and does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home.

Analysis:

The pizza chain has a legitimate interest in attempting to sell more of its products to its customers. On the other hand, there does not appear to be any significant intrusion into Claudia's privacy, or any other undue impact on her interests and rights.

The data and the context are relatively innocent (consumption of pizza). The pizza chain established some safeguards: only relatively limited information is used (contact details) and the coupons are sent by traditional mail. In addition, an easy-to-use opportunity is provided to opt-out of marketing on the website. On balance, and considering also the safeguards and measures in place, the interests and rights of the data subject do not appear to override the legitimate interests of the pizza chain to carry out this minimal amount of data processing.

Scenario 2: targeted advertisement for the same special offer

The context is the same but the following are data are collected and processed:

- recent order history (for the past three years)
- purchase history is combined with data from the supermarket where Claudia does her shopping online
- location data is also tracked via her mobile phone
- analytics software is run through the data and predicts her preferences and the times and locations when she will be most likely to make a larger purchase, willing to pay a higher price, susceptible to being influenced by a particular rate of discount

She receives the adverts and special offers both online and off-line. Claudia is thoroughly annoyed by persistent ads popping up on her mobile phone. She was unable to find user-friendly information or a simple way to switch off these advertisements.

She was also surprised to see when she moved to a less affluent neighbourhood, that she no longer received her special offers. This resulted in an approximately 10% increase on her monthly food bill. A friend showed her some speculations in an online blog that the supermarket was charging more for orders from 'bad neighbourhoods', on grounds of the statistically higher risks of credit card fraud in such cases. The company did not comment and claimed that their policy on discounts and the algorithm they are using to set prices are proprietary and cannot be disclosed.

Scenario 2: targeted advertisement for the same special offer



Analysis:

The data and the context remain of relatively innocent nature. However, the scale of data collection and the techniques used to influence Claudia are factors to be considered when assessing the impact of the processing.

Lack of transparency about the logic of the company's data processing that may have led to de facto price discrimination based on the location where an order is placed, and the significant potential financial impact on the customers ultimately tip the balance even in the relatively innocent context of take-away foods and grocery shopping.

Instead of merely offering the possibility to opt-out of this type of profiling and targeted advertisement, consent would be necessary. As a consequence, legitimate interest should not be relied on as a legal ground for the processing.

Scenario 3: use of food orders to adapt health insurance premiums

Claudia's pizza consumption habits, including the time and nature of food orders, are sold by the chain to an insurance company, which uses them to adapt its health insurance premiums.

Analysis:

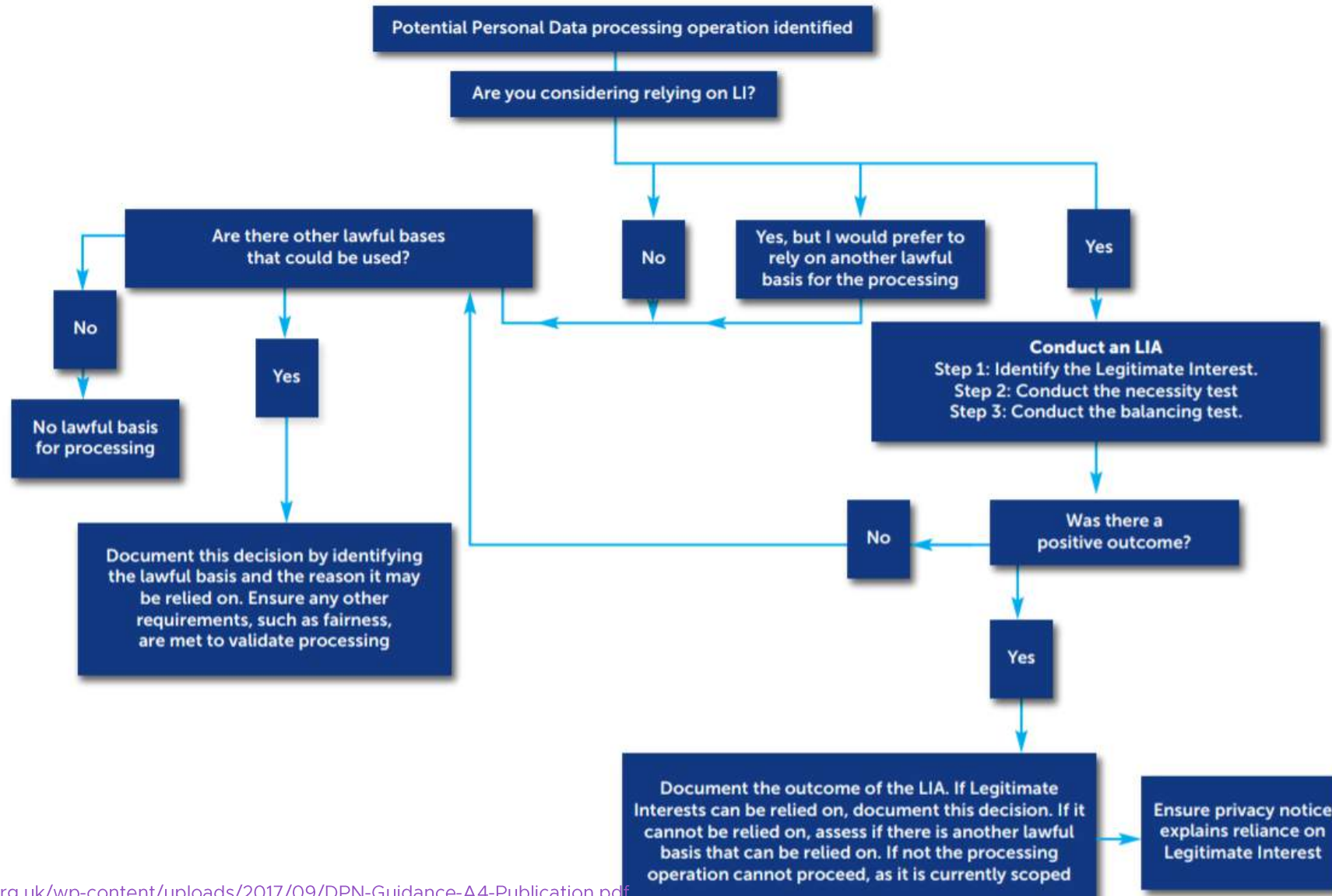
The health insurance company may have a legitimate interest - to the extent applicable law allows this - in assessing the health risks of its customers and charge differentiated premiums according to the different risks.

However, the way in which the data are collected and the scale of the data collection in itself are excessive. A reasonable person in the situation of Claudia would be unlikely to have expected that information about her pizza consumption would have been used to calculate her health insurance premiums.

In addition to the excessive nature of the profiling and possible inaccurate inferences (the pizza could be ordered for someone else), the inference of sensitive data (health data) from seemingly innocuous data (take-away-orders) contributes to tipping the balance in favor of the data subject's interests and rights. Finally, the processing also has a significant financial impact on her.

On balance, in this specific case the interests and rights of the data subject override the legitimate interests of the health insurance company. As a consequence, legitimate interest should not be relied on as a legal ground for the processing.

Legitimate Interests Assessment



COMMISSION

Thank you!

PROPERTY OF

