Auteur: Jelle Slotman is Senior Security Consultant bij Sogeti Nederland en onlangs als Master afgestudeerd aan de Hogeschool Utrecht. Hij is te bereiken onder jelle.slotman@tutanota.com. Dit artikel is een excerpt van de master scriptie van de Master of Informatics aan de Hogeschool Utrecht dd. november 2022.

Dark patterns in cookie consent notices

Wie regelmatig surft op het internet wordt doodgegooid met allerlei cookie verzoeken. Waar 'cookie consent notices' ooit zijn bedacht om de eindgebruiker te voorzien van zelfbeschikking en transparantie, lijkt het alsof websites alle mogelijkheden aanwenden om het tegenovergestelde te bereiken door het gebruik van 'dark patterns'. In dit artikel wil ik de lezer meenemen in de door mij uitgevoerde studie en de mogelijke oplossing voor een ethisch 'cookie consent design'.

Wat zijn cookies en wat is het probleem?

Web services gebruiken cookies voor het volgen van gebruikers met verschillende doeleinden. Cookies zijn kleine bestanden die het volgen van gebruikers mogelijk maakt. Zo kunnen webshops door middel van cookies een digitale winkelwagen of (anonieme) analytics bijhouden over het gebruik van de website. Deze cookies worden functionele of analytische cookies genoemd. De kern van eerder genoemde verwerkingen is dat deze anoniem zijn. Echter, als de gebruiker geïdentificeerd kan worden dan dient deze goedkeuring te geven in lijn met de Privacy richtlijn 2002 (ook wel bekend als de cookiewet) en de Algemene Verordening Gegevensbescherming (AVG).

Dit kan bijvoorbeeld gaan om verwerking voor bepaalde marketing activiteiten of het bijhouden van data om de gebruiker een gepersonaliseerd beeld te geven. Het belangrijkste punt hierbij is dat de website de gebruiker voldoende middelen geeft om op een geïnformeerde wijze een besluit te kunnen maken over de verwerking van persoonsgegevens.

Dit is precies het punt waar het in de praktijk verkeerd gaat. Verschillende studies binnen het praktische en wetenschappelijke domein hebben aangetoond dat veel websites gebruikmaken van verschillende visuele of tekstuele implementaties van het geven van een 'consent' om te bereiken dat de eindgebruiker zo snel mogelijk op de 'accept all cookies' klikt. Deze implementaties worden ook wel 'dark patterns' genoemd. Dark patterns zorgen ervoor dat het gebruikers (nagenoeg) onmogelijk gemaakt wordt om geïnformeerde beslissingen te nemen over het verwerken van persoonsgegevens. Een voorbeeld is te vinden in figuur 1, weergave van de website van gereedschapcentrum.nl (24-01-2023).

Figuur 1, bron: gereedschapscentrum.nl.

Er zijn een paar dingen die de gebruiker bijna dwingen tot accepteren. Als eerste valt op dat het lijkt alsof je de cookies alleen maar kunt accepteren door op de groene

Dark pattern	Description
Presentation	The desired choice is highlighted (e.g., color, text) in such a way that users may oversee other options.
Forced action and timing	The user is forced into a certain action on the spot.
Understanding mapping	Mapping information makes it difficult to evaluate into familiar evaluation schemes
Providing feedback	Feedback is used to steer users into the desired choice.
Providing Incentives	Incentives are used to reward the desired choice.
Expecting Error/Reversibility	Expecting users to make errors and being as forgiving as possible
Overly complex or easy information or structures	Information or information structures are either too simple or complex and hidden so that users are unable to provide their informed consent.
Bad defaults	Specific defaults are used by the company in the hope users do not decline them.

Tabel 1

button te klikken. Echter, bij het lezen van de tekst blijkt er wel de mogelijkheid om te weigeren, al wordt de gebruiker overduidelijk gestuurd om op de button te klikken en impliciet alle cookies te accepteren. Hoewel dit slechts een klein voorbeeld is, zijn er legio verschillende manieren om gebruikers te beïnvloeden. De irritatie die dit bij mij opwekte heeft er uiteindelijk voor gezorgd dat ik deze patronen (of patterns) ben gaan bestuderen en daarmee verandering hoop te brengen in het huidige klimaat. Dit heb ik gedaan door een lijst criteria op te stellen die zorgen voor een ethisch verantwoorde en GDPR compliant cookie consent notice.

Uitvoering van de studie

De uitgevoerde studie is gebaseerd op de Design Science methodologie van Peffers. Dit is een wetenschappelijke benadering voor het uitwerken van een design artefact en leent zich uitstekend voor het ontwikkelen van de checklist. De in het onderzoek gebruikte methodologie is opgebouwd uit vijf stappen, te weten: het definiëren van het probleem, het definiëren van de oplossing, het ontwikkelen van de oplossing, demonstratie van het artefact en het communiceren van de resultaten.

- *Definiëren van het probleem en definiëren van de oplossing*
  Door middel van literatuurstudie in professionele en wetenschappelijke context is de probleemstelling opgesteld. Uit het onderzoek is gekomen dat er op het moment een disconnect heerst tussen **compliance** en **ethiek**. Ethische richtlijnen voor gebruik van dark patterns zijn onvoldoende meegenomen en geven onvoldoende richtlijnen om 'informed consent' mogelijk te maken.
  Om bovenstaand probleem op te lossen zou er een checklist moeten komen die ervoor zorgt dat een cookie consent notice compliant is en dark patterns voorkomt. Door gebruik van het anti-pattern zou een weg naar ethisch cookie consent mogelijk gemaakt moeten worden.

- *Design en development van de checklist*
  De basis voor de checklist is een lijst van items uit de AVG guidelines (consent en transparantie) die samen het geheel aan richtlijnen toont. Deze lijst vormde een opsomming van alle vereisten die gesteld worden door de Europese commissie. Vervolgens is er op basis van wetenschappelijk onderzoek een specifieke lijst met dark patterns (tabel 1) gevonden, die van toepassing zijn op consent.

De eerste versie van het model is bereikt door een mapping uit te voeren van de dark patterns op de lijst met compliance criteria. Deze gezamenlijke lijst heeft tot de eerste versie van de checklist geleid.

Tabel 2 toont de checklist items met daarbij het/de relevante dark pattern(s).

Basic requirements		
Requirement (compliance criteria)	**Notes**	**Related Dark pattern(s)**
(1) The consent notice doesn't block users from accessing the website.	Consent is not blocking, ensuring that consent is freely given.	Forced action and timing
(2) Consent is required, besides cookies (strictly) necessary for communication, for servicing the user, and/or to obtain information about the quality and/or efficiency of the service. (3) No information is processed before consent is obtained.		
(4) A layered and standardized approach is used for different types of consent (e.g. basic advertisement, market research).		Overly complex or easy information or structures
(5) Consent is only obtained through a clear and affirmative action (no pre-checked boxes).		Bad defaults
(6) The following information is presented in the notice (link to the privacy policy is allowed): 1. The controller's identity. 2. The purpose for each of the processing operations where consent is sought. 3. What data will be collected and used. 4. How users may withdraw their consent at any time. 5. Information about the use of data for automated decision-making. 6. (Where relevant) inform the user of the risk of data transfers out of the territorial scope.		
(7) All consent is logged in order to demonstrate user consent.		
(8) Withdrawing consent is as easy as providing it.		
(9) Processing stops immediately, and stored information is deleted after user has withdrawn consent.		

Requirements for communication toward the data subject		
Requirement	**Notes**	**Related Dark pattern(s)**
(10) Privacy-related communications are clearly distinguishable from non-privacy-related information.	Communications must be concise, transparent intelligible, and easily accessible (art. 12(1) GDPR)	Overly complex or easy information or structures
(11) The entity uses communications understandable by an average member of the target audience.	Intelligible communications	

Requirements for communication toward the data subject		
Requirement	**Notes**	**Related Dark pattern(s)**
(12) The user should be able to determine in advance the scope and consequences of the processing (no surprises afterward).		Overly complex or easy information or structures
(13) The presented information makes it immediately clear how users can access their personal data.	Information is easily accessible.	
(14) Users are not steered towards desired choices through the use of feedback, incentives, and/or reversible actions (e.g., error messages).		Providing feedback, Providing Incentives, Expecting Error/Reversibility

Language/readability requirements for clear and plain language toward the data subject		
Requirement (grey text is used as a recommended requirement)	**Notes**	**Related Dark pattern(s)**
(15) Use sentences with a maximum of 20 words and use as many simple words as possible.		Overly complex or easy information or structures
(16) Active language is used to improve the directness of the message		Overly complex or easy information or structures
(17) No false friends*, jargon, and abbreviations are used, especially for websites over multiple languages *Words in different languages that look or sound the same but have different meanings.		Overly complex or easy information or structures
(18) Icons and visualizations may be used to strengthen the message. However, the icons/visualizations may not replace the written message. Highlighting visualizations or text is highly forbidden.		Presentation

Requirements when addressing offering services where children and/or vulnerable people may be the audience		
Ethical compliant requirement	**Notes**	**Related Dark pattern(s)**
(19) When addressing vulnerable people or children, use vocabulary, tone, and style so that the children know that the information is directed to them.		
(20) Seek an appropriate manner to provide transparency to vulnerable persons (physical/mental disability).		

Tabel 2

Deze eerste checklist is voorgelegd aan een panel van security/privacy specialisten (n=10), waarbij de bruikbaarheid van de items is getoetst en een rangschikking is gemaakt op basis van de belangrijkheid voor cookie consent design. Dit leverde een gevalideerde en gerangschikte lijst op, die aan de hand van een case is voorgelegd aan twee design specialisten.

- *Demonstratie*
  Het doel voor de onderzoeksfase was het demonstreren van het artefact in een praktische situatie (n=2). De demonstratie leverde feedback op ter verbetering van het artefact. Hierbij is voornamelijk gefocust op het opstellen van guidelines ter verduidelijking van de checklist. Verder is aan de hand van feedback discussie op de resultaten gevoerd.
- *Eindresultaat*
  Het uitvoeren van de studie heeft geleid tot onderstaande checklist (tabel 3). De guidelines zijn beschreven op basis van de input van de design professionals en de uitkomsten van de Delphi study.

Criterion	Guidelines
The consent notice doesn't block users from accessing the website (e.g. cookie wall).	1. There is a difference between public (open) and private (paid) services. For private services, a wall may be implemented prohibiting users to access the (private) website. 2. For the processing of personal information where consent is used as the basis of processing, the consent notice is still obligated. Cookie walls are prohibited.
Consent is only obtained through clear and affirmative action (no pre-checked boxes).	1. Pre-checked consent boxes are prohibited in most cases. Website users should have the autonomy to choose what personal information is processed from them. 2. Pre-checked boxes can only be used when certain processing activities rely on legitimate interest. 3. Specific color schemes can be used but these should be there to assist in making informed choices.
Withdrawing consent is as easy as providing it.	1. Withdrawing consent does not have to be done through the use of cookie banners. 2. Simple withdrawal is key.
Users are not steered towards desired choices through the use of feedback, incentives, and/or reversible actions (e.g. error messages).	1. These tricks may be used to make consent more informed. 2. An example could be to show feedback on processing consequences when users provide their consent. Note that this is a grey area as this also could steer website users.
When addressing vulnerable people or children, use vocabulary, tone, and style so that the children know that the information is directed to them.	1. Parents/caretakers should provide their consent. 2. Greater responsibility is necessary for situations where vulnerable persons and/or children are within your target audience.
Where consent is the basis of processing, no personal data is processed before the cookie consent is obtained.	1. Functional (e.g. tracker on shopping basket) and analytical (e.g. visitor statistics) cookies can be processed without consent. 2. Legitimate interest (when processing is necessary) is still optional for certain processing activities. Processing based on legitimate interest does not require consent.
All consent is logged to demonstrate user consent.	1. Not necessary for situations where consent is not required (legitimate interest, functional/analytical cookies)
The user should be able to determine in advance what the scope and consequences of the processing entail (no surprises afterward).	1. The consent notice should make the scope and consequences very clear. Make the message as comprehensive and compact as possible. 2. Example of this criterion would be that website users could click through the scope/ consequences per processing activity.
Seek an appropriate manner to provide transparency to vulnerable persons (physical/mental disability).	1. Also, in this context, mind that caretakers/parents need to consent on behalf of this target group. Be very strict about using language as plain and simple as possible. 2. Target group analysis helps find out how relevant this criterion is.

Criterion	Guidelines
The following information is presented in the notice (a link to the privacy policy is allowed): 1. The controller's identity. 2. The purpose for each of the processing operations where consent is sought. 3. What data will be collected and used 4. How users may withdraw their consent at any time. 5. Information about the use of data for automated decision-making. (Where relevant) inform the user of the risk of data transfers out of the territorial scope.	1. The information may also be provided through references (links etc.). 2. Use a concise version within the cookie consent notice. 3. For #2 describe who are the third parties with whom the data is shared and what is the legal basis for the activities. 4. For #3 also include how long the information will be retained. 5. Also include the contact details for the Data Protection Officer (DPO)
Presented privacy information is the same across multiple devices and device types (phone, laptop, tablet).	1. Ensure the provided information is the same across different platforms. 2. For convenience the information may be provided in a (slightly) different format if that improves comprehensibility.
Consent is required, except for cookies (strictly) necessary for communication, cookies necessary for servicing the user, and cookies to obtain information about the service's quality and/or efficiency.	1. Consent may not be provided through a default 'yes' as consent is provided through a clear and affirmative action. 2. Only request consent for processing activities that need consent (everything besides functional and analytics cookies). 3. Where consent is required make it clear what the scope and consequences entail. 4. Only request the strictly necessary processing activities.
The entity uses communications understandable by an average member of the target audience.	1. An analysis of the target audience helps to find the tone and voice required for the message (e.g. education and background analysis). 2. Creativity is key when implementing these messages. E.g., videos could be used to display the message. However, a written message is obligated.
No false friends*, jargon, or abbreviations are used, especially for websites over multiple languages. *Words in different languages that look or sound the same but have different meanings	1. Only use these words if necessary. It also helps to have the target group in mind. 2. Align language use over multiple languages.
Processing stops immediately and stored information is deleted after consent is withdrawn	1. Exceptions may exist in certain salutations where legal obligations apply (e.g tax, fraud investigations, product reliability, tax laws, and medical records). Generally, these are based on another basis of processing but keep this in mind. 2. It is not forbidden to anonymize after consent is withdrawn. For more details art. 29 WP216 provides the guidelines for proper anonymization techniques.
The presented information makes it immediately clear how users can access their personal data.	1. This could be done through a link or other means where users can see what data is processed by the organization. 2. The information could also be presented in the privacy statement.
Use sentences with a maximum of 20 words and use as many simple words as possible.	1. 6-8-year-old children should be able to understand this message. 2. E.g. uses B1 language, which is also used for Dutch government communications. 3. Align the message to the target audience.

Criterion	Guidelines
Active language is used to improve the directness of the message.	1. Active language uses verbal forms (to do) instead of passive voice using combinations (have done). 2. In combination with a limited word count the directness and ease of the message improve greatly. 3. Look at the message from a communication perspective instead of a legal perspective.
A layered and standardized approach is used for separating multiple consent requests (e.g. basic advertisement, market research).	1. Make it transparent for each processing activity when, and where, consent is provided. This enables users to make their own choices based on the information. 2. Make the requests as simple and concise as possible. 3. With layered is meant that website users should be presented with different categories that require consent. Each separate category should receive separate consent.
Icons and/or visualizations may be used to strengthen the message. Icons and/or visualizations may not replace the written message. Highlighting visualizations or text is highly forbidden.	1. Icons/visualizations should never replace text. The use of text is obligatory. 2. Highlighting is forbidden if this steers users towards the desired behavior. Highlighting may be used to improve the understandability of the message.
The cookie consent notice only includes communications necessary to explain the data subject for what purposes consent is requested. Other information may be provided through references and/or links.	1. Other information is all non-privacy-related information. 2. For cookie banners the purposes of processing are important to explain. Other information could also be described in the privacy statement.

Tabel 3

De studie heeft een goede eerste versie geleverd voor de checklist. Met bovenstaande checklist kunnen design professionals een cookie consent notice beschrijven op basis van de criteria. Hoewel er een aantal praktische uitdagingen zijn met betrekking tot het gebruikte jargon en de structuur van de checklist, kan dit artefact als succesvol en bruikbaar bestempeld worden.

Opmerkingen en aanbevelingen

Naast aanpassingen qua structuur en jargon, is een aanbeveling voor vervolgonderzoek om de demonstratiefase uit te voeren met een bredere 'sample group'. Dit zou ertoe kunnen leiden dat de checklist bruikbaarder wordt voor verschillende doelgroepen. Verder is het vervalmoment van consent een terugkerend thema geweest binnen de studie, waarbij zowel binnen de Delphi studie als bij de demonstratie genoemd werd dat een gegeven consent niet voor altijd zou moeten zijn. Vervolgonderzoek zou kunnen uitwijzen of dit een relevant thema is en op welke wijze het vervalmoment van consent geïmplementeerd kan worden.

Afsluitend is er in de praktijk een ontwikkeling te bemerken als het gaat om cookie consent. Waarbij in de 'oude' situatie voornamelijk gebruik werd gemaakt van een doorzichtige implementatie van de 'bad defaults' (zie ook de tabel 1 met dark Patterns) is er in het veld te zien dat steeds meer websites gebruikmaken van de 'legitimate interest', welke default op aan staat.

Hoewel er voor marketing speciale wetten gelden binnen de AVG, valt hier vooral de niet-transparante wijze op met als doel zo veel mogelijk data te vergaren.

Vervolgonderzoek zou kunnen focussen op hoe groot het huidige probleem van onjuist gebruik van legitiem belang is en voorstellen kunnen doen om de huidige regels duidelijker te kunnen stellen. Dit zorgt voor verbetering van de checklist en zorgt ervoor dat eindgebruikers zonder beïnvloeding keuzes kunnen maken over de verwerking van persoonsgegevens.