

slideShare  
a Scribd company

Search

Upload Download free for 30 days Login

## Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors

Sep 11, 2020 • 2 likes • 893 views

J JamieWilliams130 [Follow](#)

The document discusses enhancing ATT&CK data sources by developing data models. It proposes opportunities like addressing lack of context, redundancy, and broad scope in ATT&CK data sources. It then describes a process to model adversary behavior li... [Read more](#)

1 of 66 [Download to read offline](#)

1 Started From the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors

2 Agenda

3 ATT&CK Data sources?

4 When we introduce a threat... Introducing Blue Mockingbird

5 Threat modeling

6 Threat modeling

7 Threat modeling

8 Threat modeling

9 Threat modeling

10 Threat modeling

11 Threat modeling

12 Threat modeling

13 Threat modeling

14 Introducing Blue Mockingbird

15 Are ATT&CK data sources sufficient for security operations?

16 How do data sources support this process?

17 Any opportunities for ATT&CK data source improvement?

18 Some opportunities for improvement are...

19 Opportunity: Lack of context

20 Opportunity: Redundancy and overlapping

21 Opportunity: Too broad scope

# Started From the Bottom: Exploiting Data Sources to Uncover ATT&CK® Behaviors

Jose Rodriguez @Cyb3rPandaH  
Jamie Williams @jamieantisocial  
MITRE ATT&CK @MITREattack



©2020 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 20-00876-8.

## Agenda

- Data sources?
- Are ATT&CK data sources sufficient for security operations?
  - Any opportunities for ATT&CK data sources improvement?
  - How can we enhance current data sources?
  - How do these concepts apply to ATT&CK?
- Data-driven hunt experiment



### Recommended

Lateral Movement wi... kieranjacobsen

Android malware ... Jason Ross

Outlook and Exchange for ... Nick Landers

Hunting for Credentials ... Teymur Kheirkhabarov

A Case Study in Attacking ... Will Schroeder

BriMor Labs Live Respons... BriMorLabs

Android malware ... Sandeep Joshi

File security system ÁSHÍYÁ ŽÂBÊÊÑ

FireEye Use Cases — ... Valery Yelain

Windows Ağlarda Saldır... Sparta Dilisim

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)  
[Third Parties](#)

[Manage Preferences](#)

[Accept All](#)

[Reject All](#)

Storage  Targeted Advertising  Personalization  Analytics

28 Documenting data sources via data dictionaries

29 How do these concepts apply to ATT&CK?

30 Adding metadata to ATT&CK data sources

31 Identifying relevant data via data source objects

32 Identifying relevant data via data source objects

33 PERSISTENCE Data-driven hunt experiment

34 A basic detection research process

# Data sources? 🤔

Tactics: Persistence, Privilege Escalation, Defense Evasion  
Platforms: Windows  
Permissions Required: Administrator, User  
**Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows Registry**  
Contributors: Jesse Brown, Red Canary  
Version: 1.0  
Created: 24 June 2020  
Last Modified: 26 June 2020

©2020 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 20-00876-8.

Masahiko Sawada

The Travelling Pentester: ...

Will Schroeder

Android security

Mobile Rtpl

Recon for Bug ...

When you hear about a new threat....

## Introducing Blue Mockingbird

Red Canary Intel is monitoring a potentially novel threat that is deploying Monero cryptocurrency-mining payloads on Windows machines at multiple organizations.

**As defenders, what can we do?**

### Threat modeling

#### Gaining entry

In at least two incident response (IR) engagements, Blue Mockingbird has **exploited public-facing web applications (T1190: Exploit Public-Facing Application)** that implemented Telerik UI for ASP.NET AJAX. This suite of user interface components accelerates the web development process, but some versions are susceptible to a deserialization vulnerability, [CVE-2019-18935](#). The exploitation of this CVE is not unique to Blue Mockingbird, but it has been a common point of entry.

In exploiting this vulnerability, two DLLs are uploaded to a web application running on a Windows IIS web server. In telemetry, investigators will notice `w3wp.exe` writing the DLLs to disk and then immediately loading them into memory afterward. In some cases, this will cause `w3wp.exe` to temporarily freeze and fail to successfully serve HTTP responses.

For a diagnostic to determine whether you are potentially affected by the Telerik CVE, you can search the IIS access logs for the string `POST Telerik.Web.UI.WebResource.axd`. In victim environments, our IR partners found entries similar to these:

```
2020-04-29 02:01:24 10.0.0.1 POST /Telerik.Web.UI.WebResource.axd type=rau 80 - Mozilla/5.0+ (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0 - 200 0 0 625
2020-04-29 02:01:27 10.0.0.1 POST /Telerik.Web.UI.WebResource.axd type=rau 80 - Mozilla/5.0+ (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0 - 500 0 0 46
```

Exploit Public-Facing Application

### Threat modeling

Exploit Public-

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

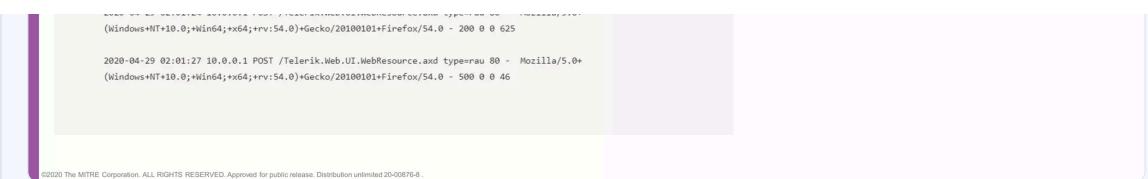
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

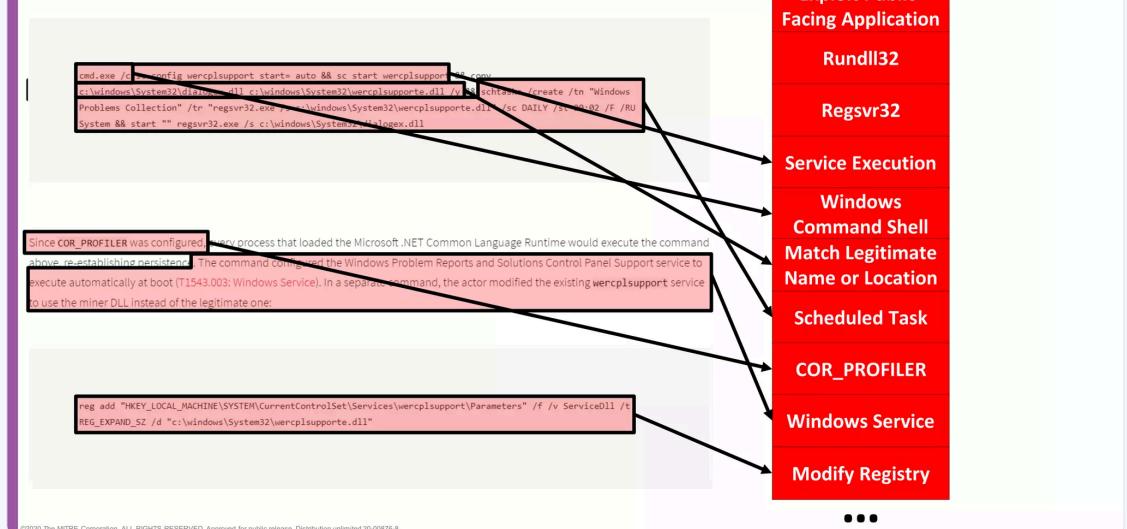
[Cookie Policy](#)

[Third Parties](#)

Storage    Targeted Advertising    Personalization    Analytics



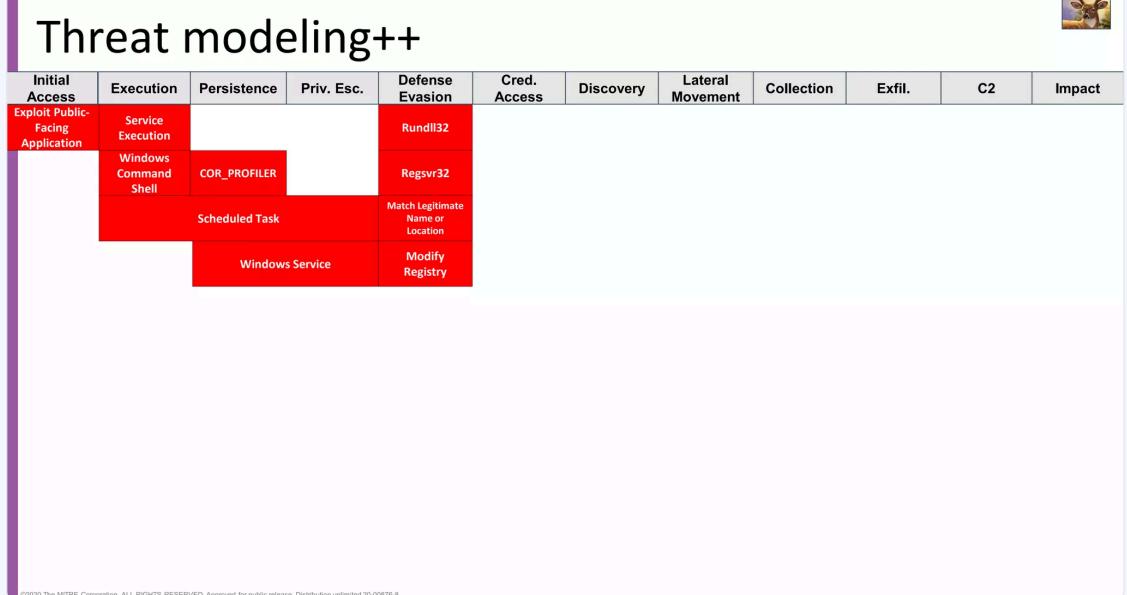
## Threat modeling



## Threat modeling++



## Threat modeling++



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage

Targeted Advertising

Personalization

Analytics

## Threat modeling++

The screenshot shows a threat modeling matrix and a detailed analysis of the Blue Mockingbird threat.

**Threat Modeling Matrix:**

Initial Access	Execution	Persistence	Priv. Esc.	Defense Evasion	Cred. Access	Discovery	Lateral Movement	Collection	Exfil.	C2	Impact
Exploit Public-Facing Application	Service Execution			Rundll32							
	Windows Command Shell	COR_PROFILER		Regsvr32							
		Scheduled Task		Match Legitimate Name or Location							
			Windows Service	Modify Registry							

**Blue Mockingbird Analysis:**

Blue Mockingbird is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were created in December 2019.<sup>[1]</sup>

**Techniques Used:**

Domain	ID	Name	Description
Enterprise	T1134	Access Token Manipulation	Blue Mockingbird has used JuicyPotato to abuse the \$asdasdasdasd token privilege to escalate from web application pool to NT AUTHORITY\SYSTEM. <sup>[2]</sup>
Enterprise	T1059 .003	Command and Scripting Interpreter: Windows Command Shell	Blue Mockingbird has used batch script files to automate execution and deployment of payloads. <sup>[3]</sup>
Enterprise	.001	Command and Scripting Interpreter: PowerShell	Blue Mockingbird has used PowerShell reverse TCP shells to issue interactive commands over a network connection. <sup>[4]</sup>
Enterprise	T1543 .003	Create or Modify System Process: Windows Service	Blue Mockingbird has made their XMRIG payloads persistent as a Windows Service. <sup>[5]</sup>
Enterprise	T1546 .003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	Blue Mockingbird has used msasn1.dll to establish WMI Event Subscription persistence mechanisms configured from a *msf* file. <sup>[6]</sup>
Enterprise	T1190	Exploit Public-Facing Application	Blue Mockingbird has gained initial access by exploiting CVE-2019-18935, a vulnerability within Telerik UI for ASP.NET AJAX. <sup>[7]</sup>
Enterprise	T1574 .012	Hijack Execution Flow: COR_PROFILER	Blue Mockingbird has used wmic.exe and Windows Registry modifications to set the COR_PROFILER environment variable to execute a malicious DLL whenever a process loads the .NET CLR. <sup>[8]</sup>
Enterprise	T1036 .005	Masquerading: Match Legitimate Name or Location	Blue Mockingbird has masqueraded their XMRIG payload name by naming it wercplusport.dll after the legitimate wercplusport.dll file. <sup>[9]</sup>
Enterprise	T1112	Modify Registry	Blue Mockingbird has used Windows Registry modifications to specify a DLL payload. <sup>[10]</sup>

**ATT&CK® Navigator Layers:**

A yellow hand icon points to the "Techniques Used" section of the table.

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

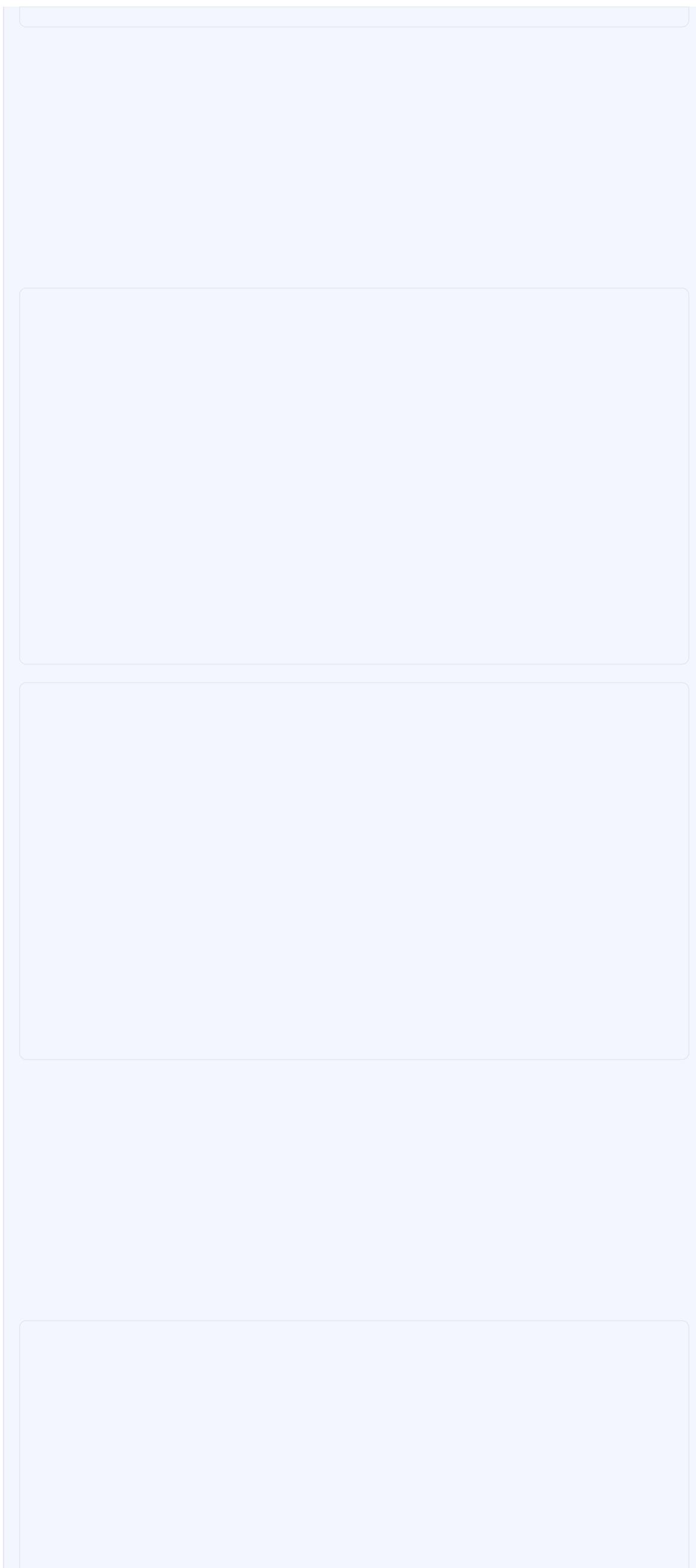
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

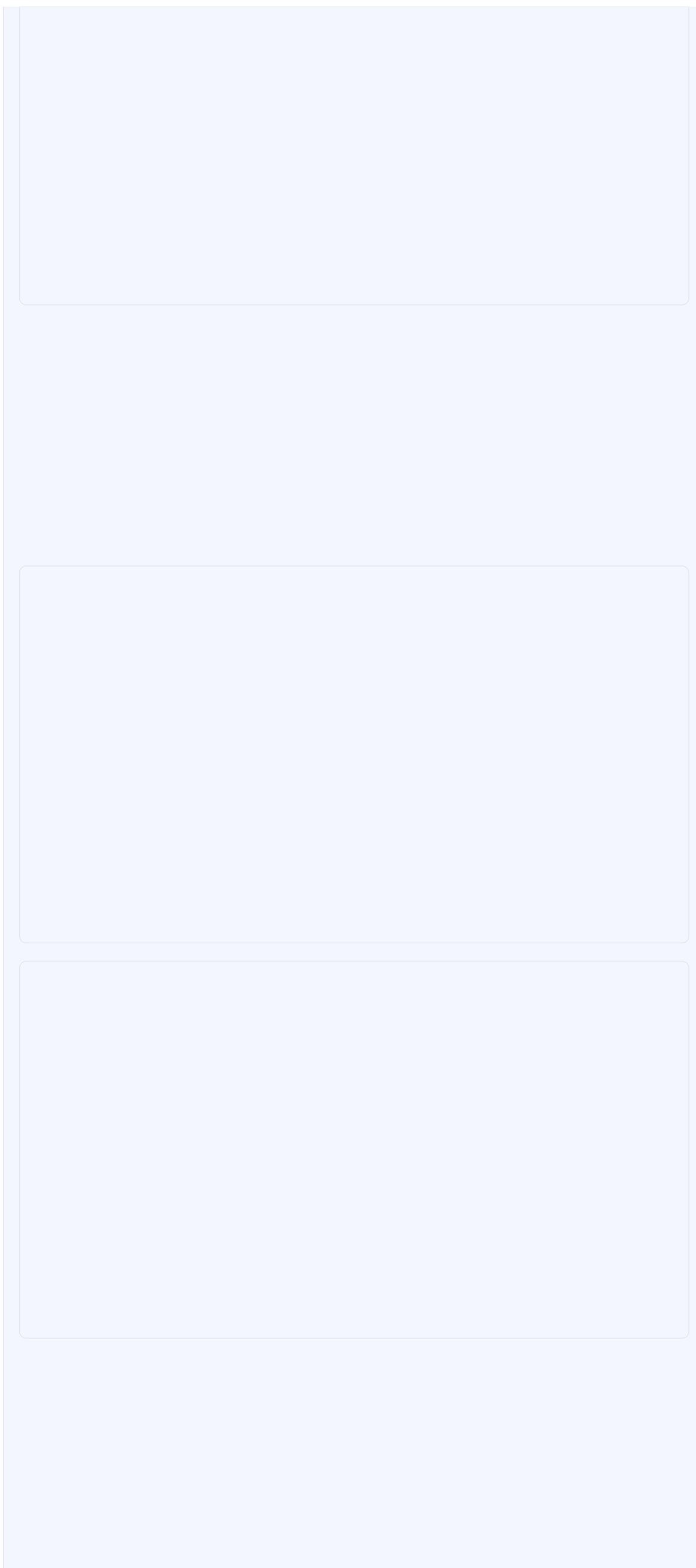
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

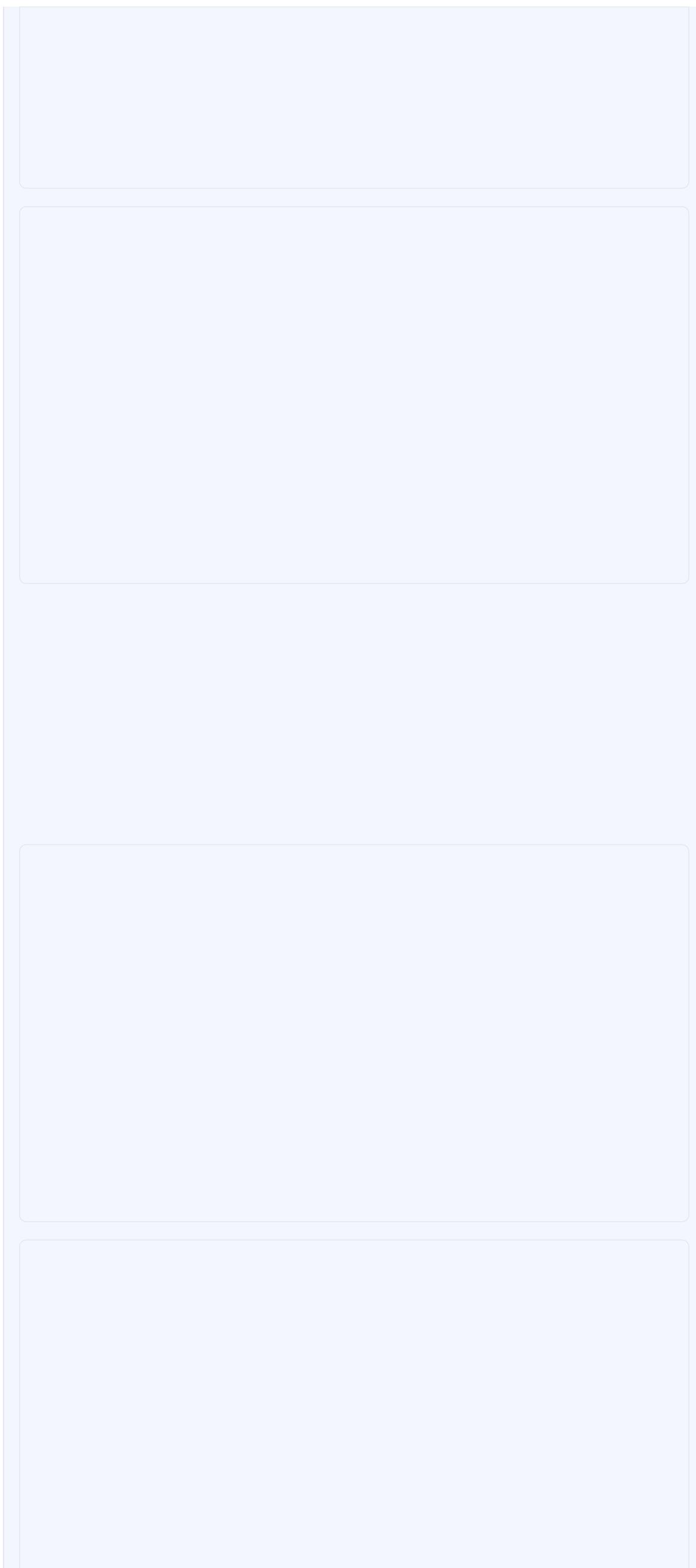
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

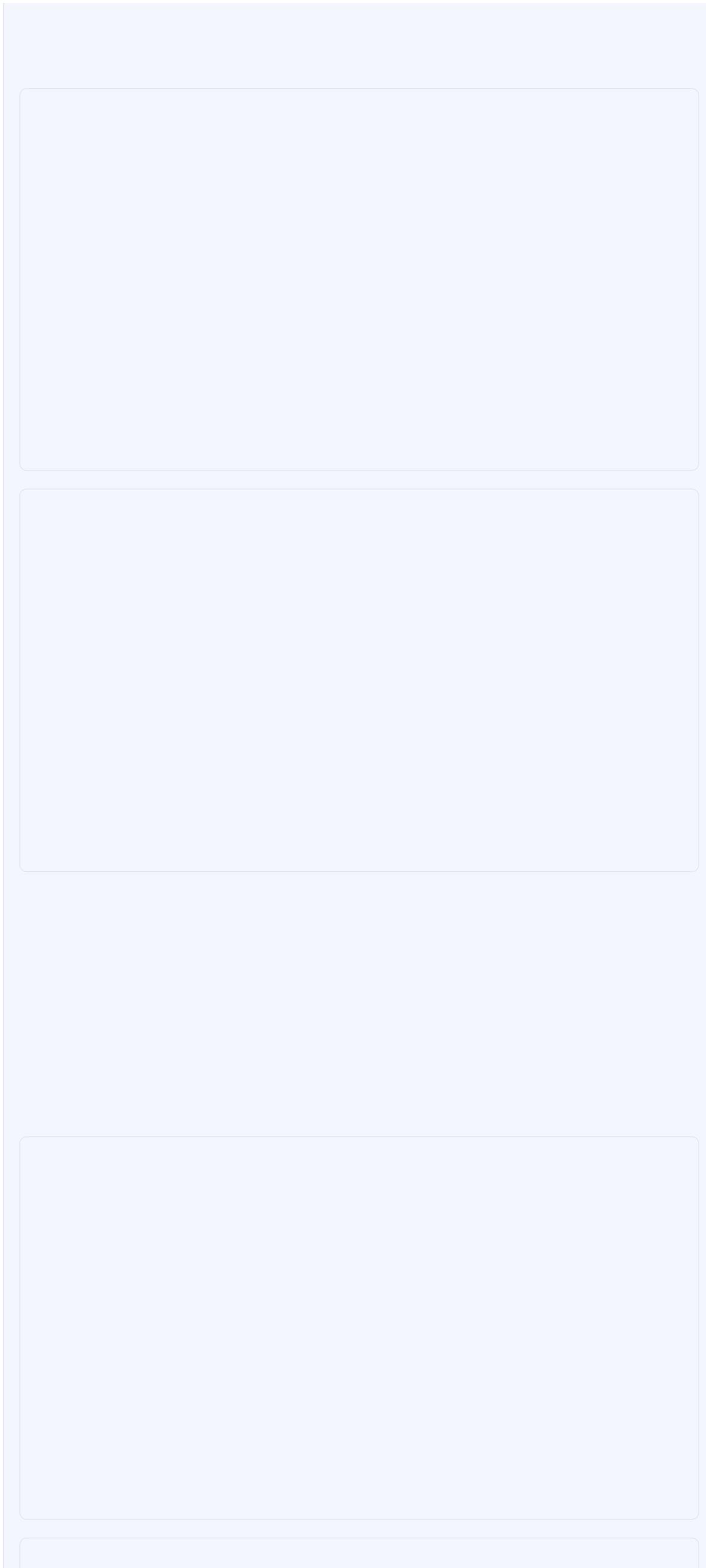
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

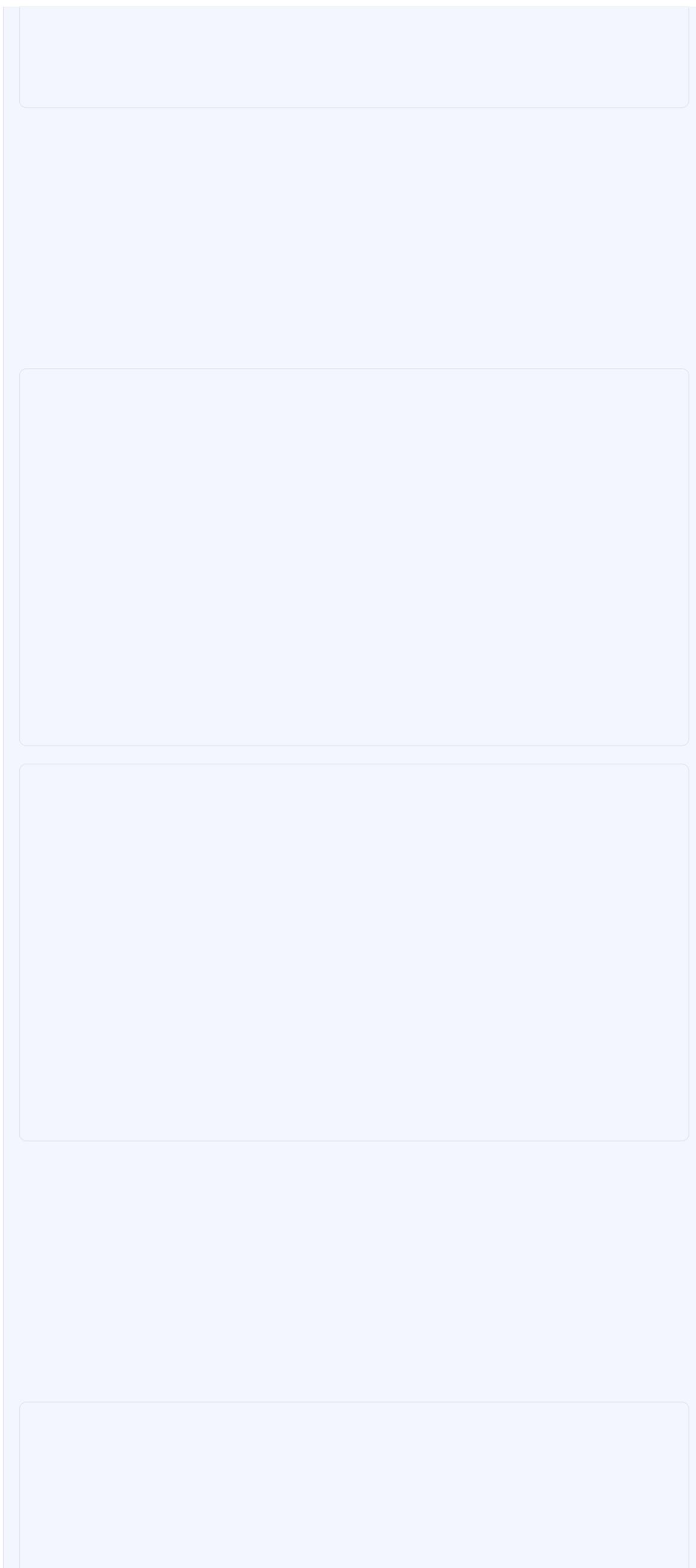
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

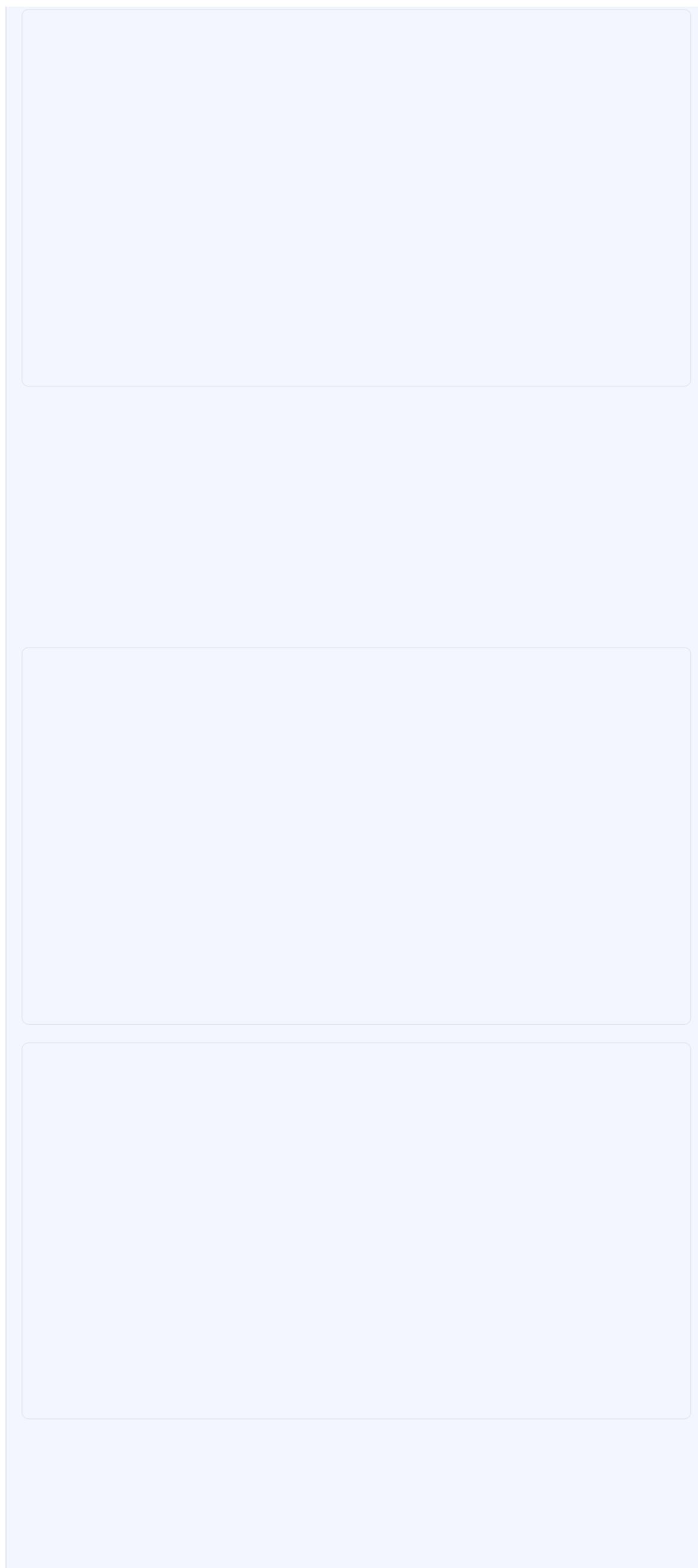
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

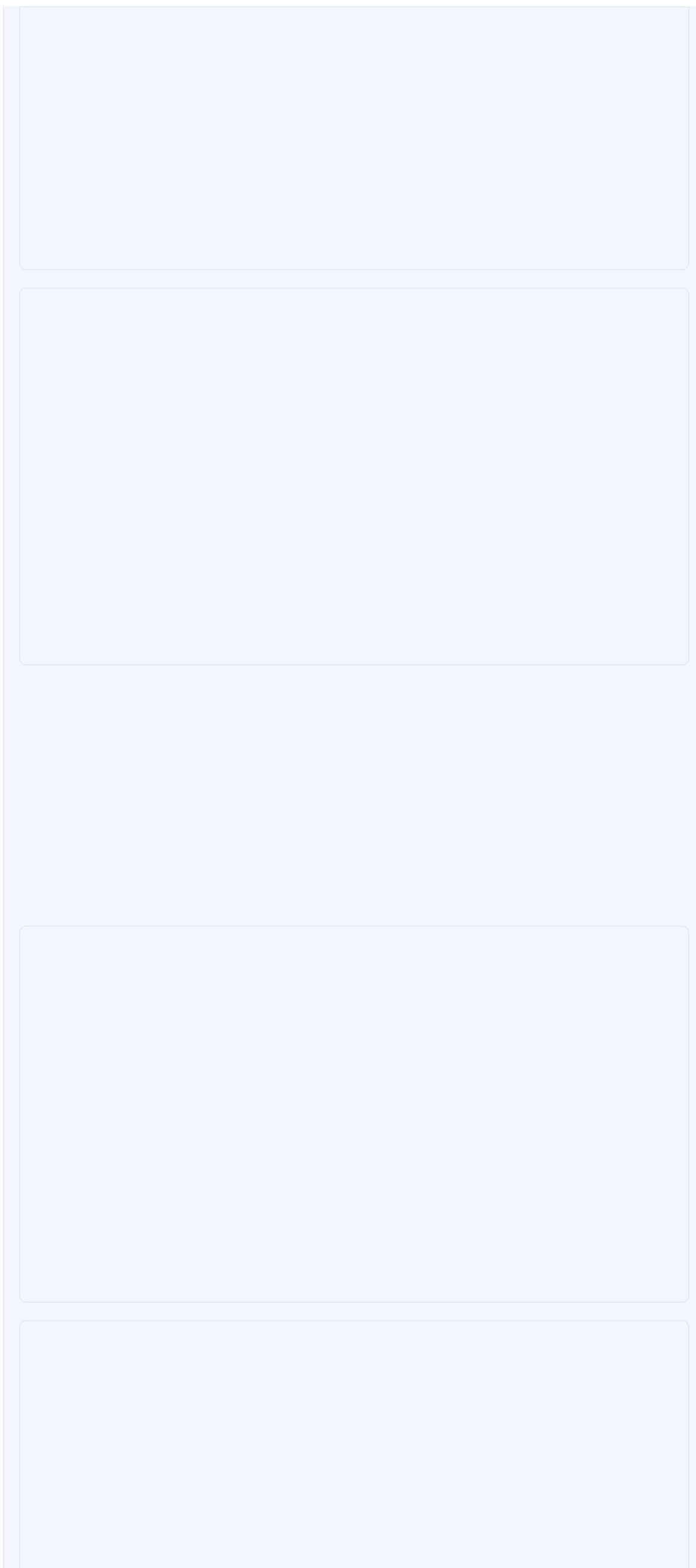
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

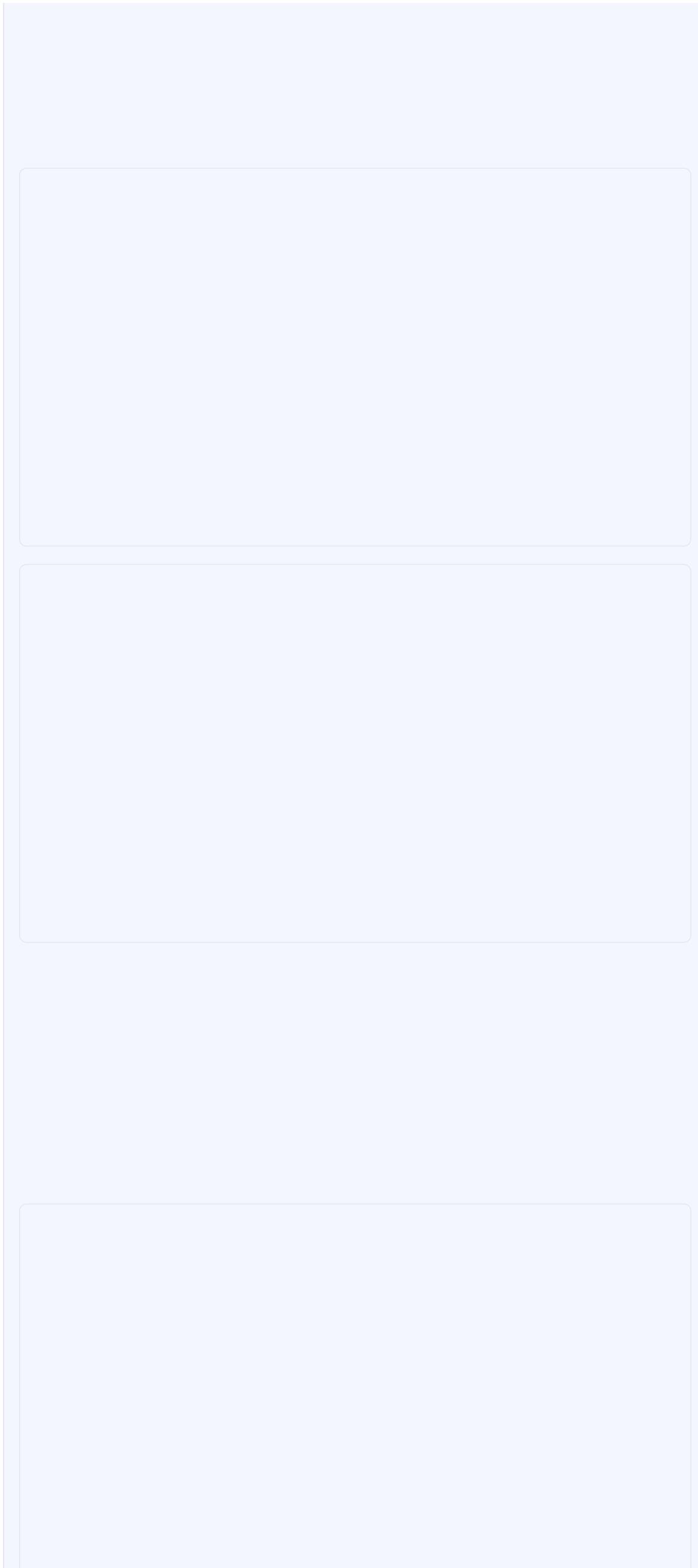
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

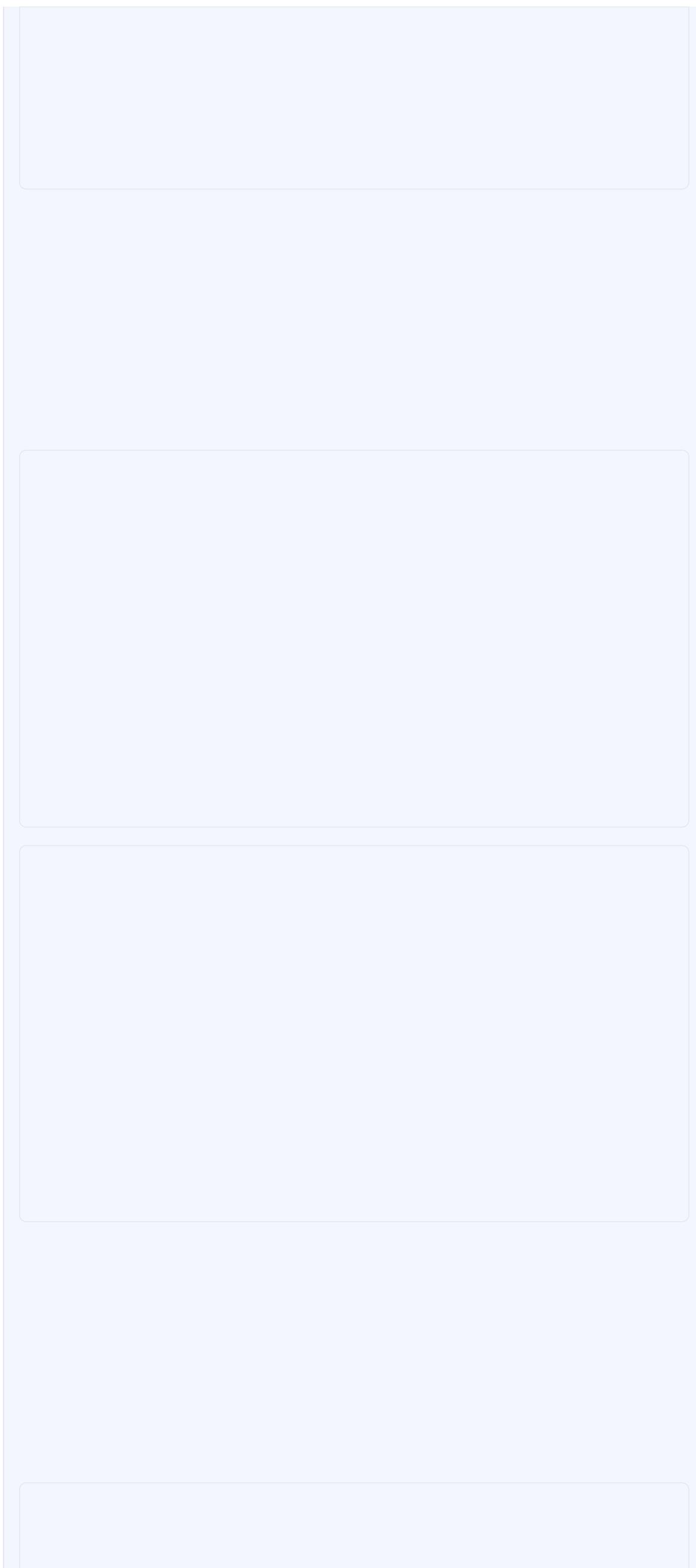
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

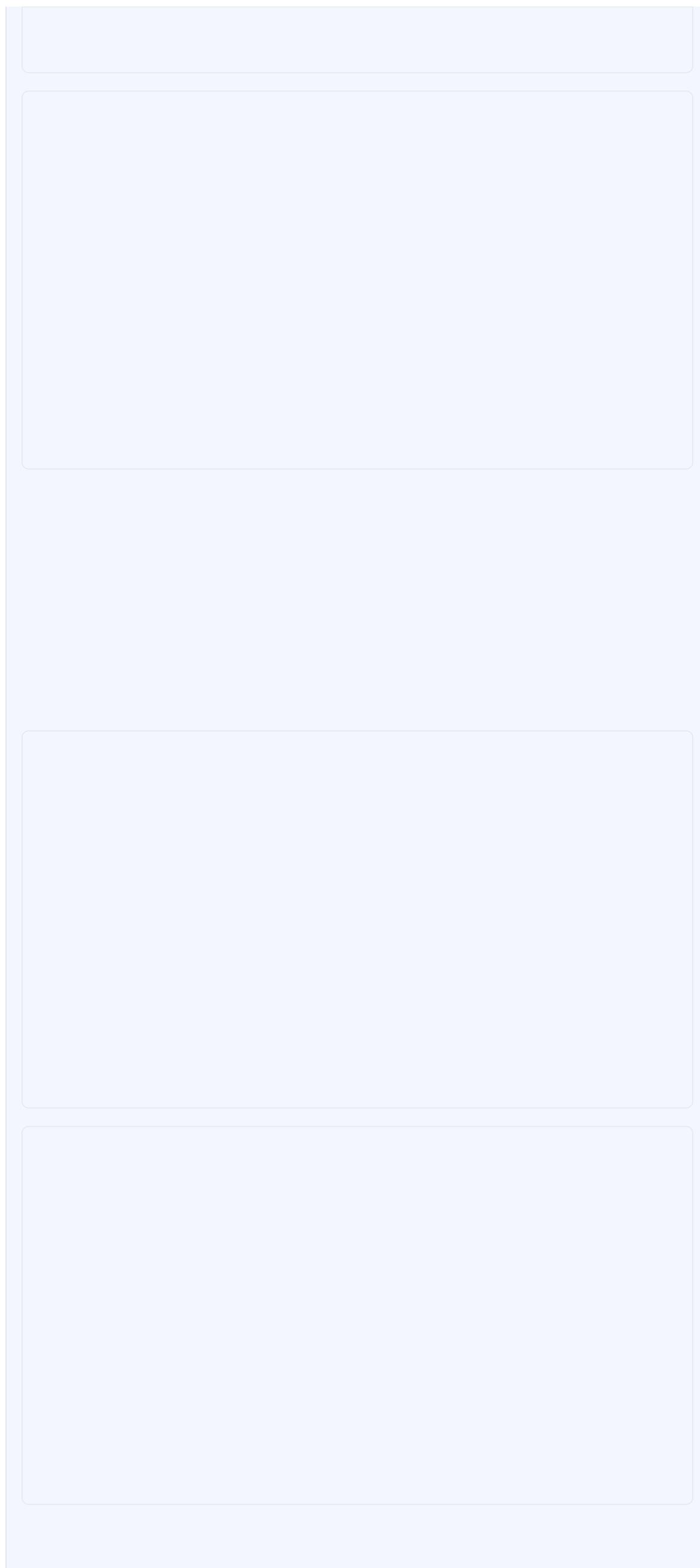
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

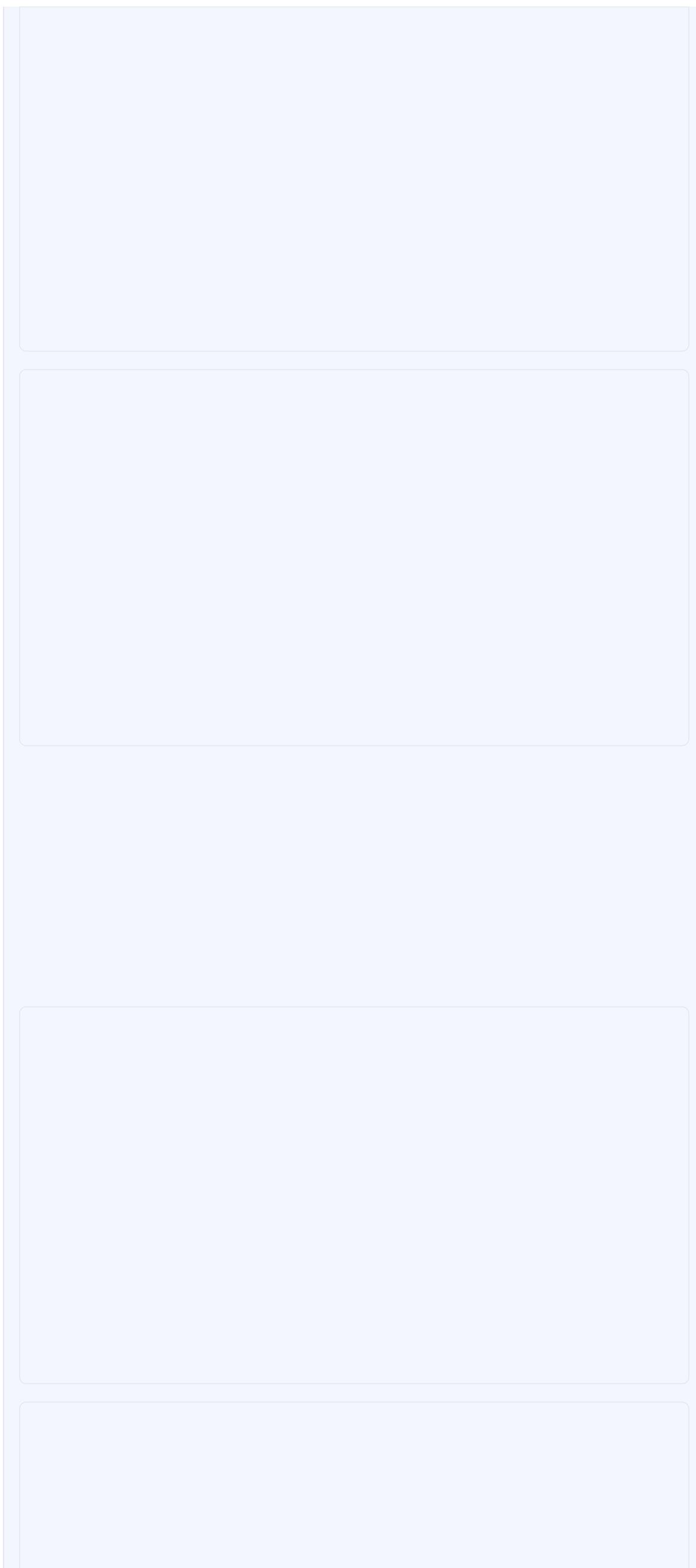
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

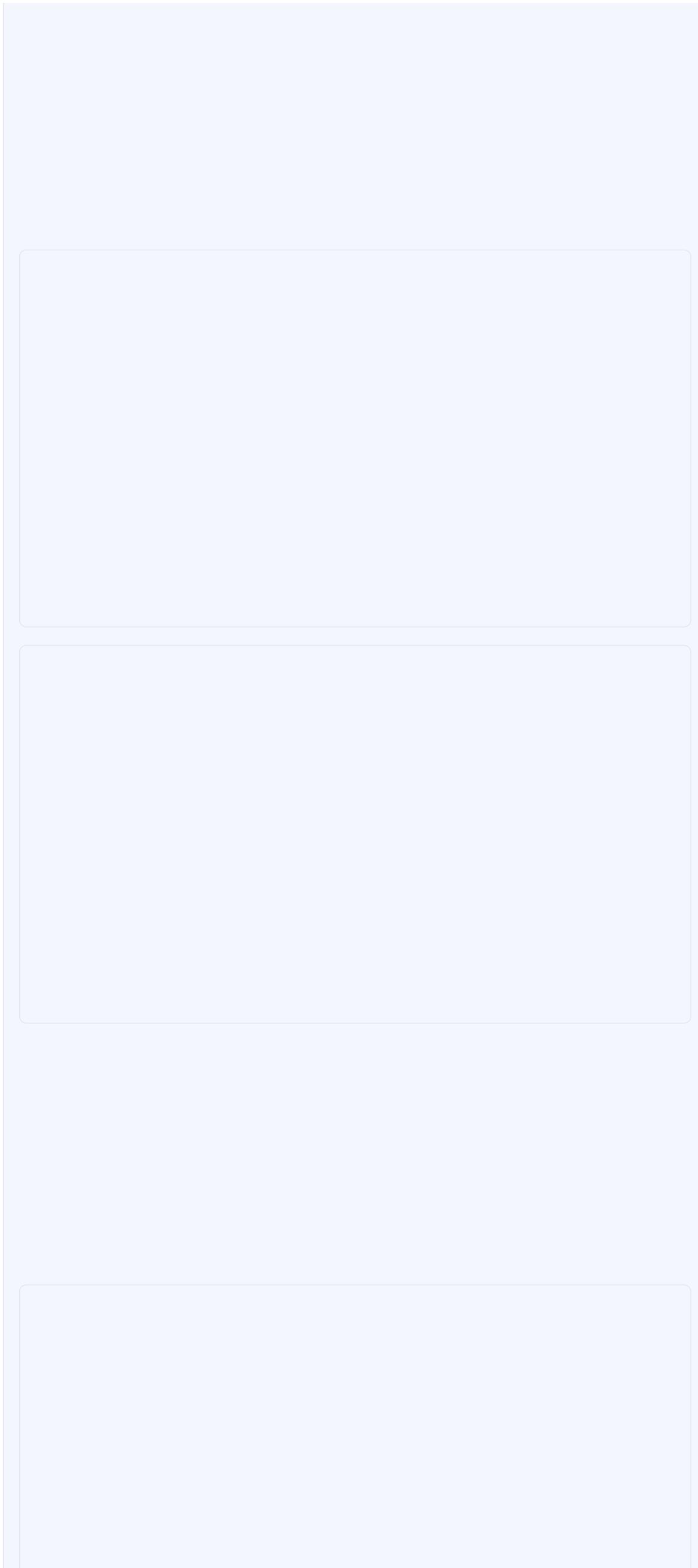
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

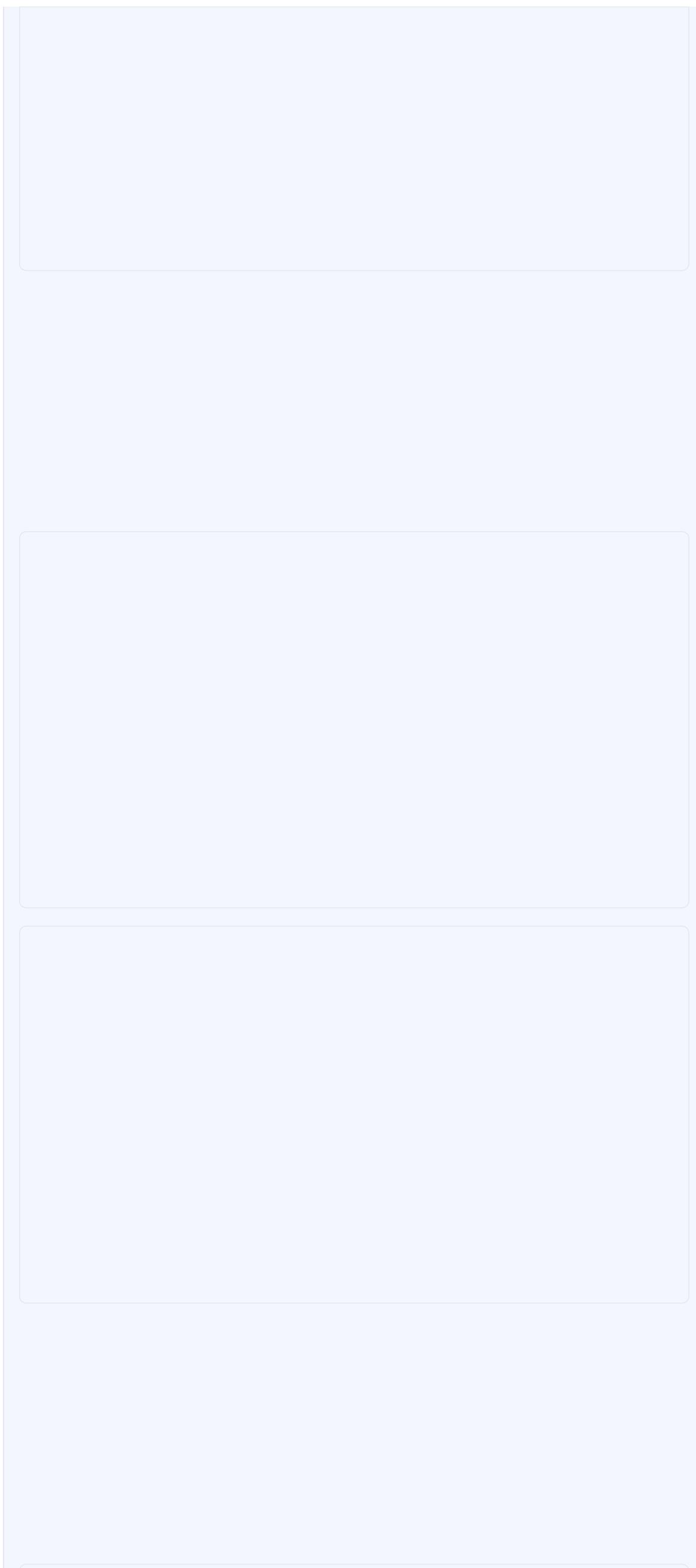
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

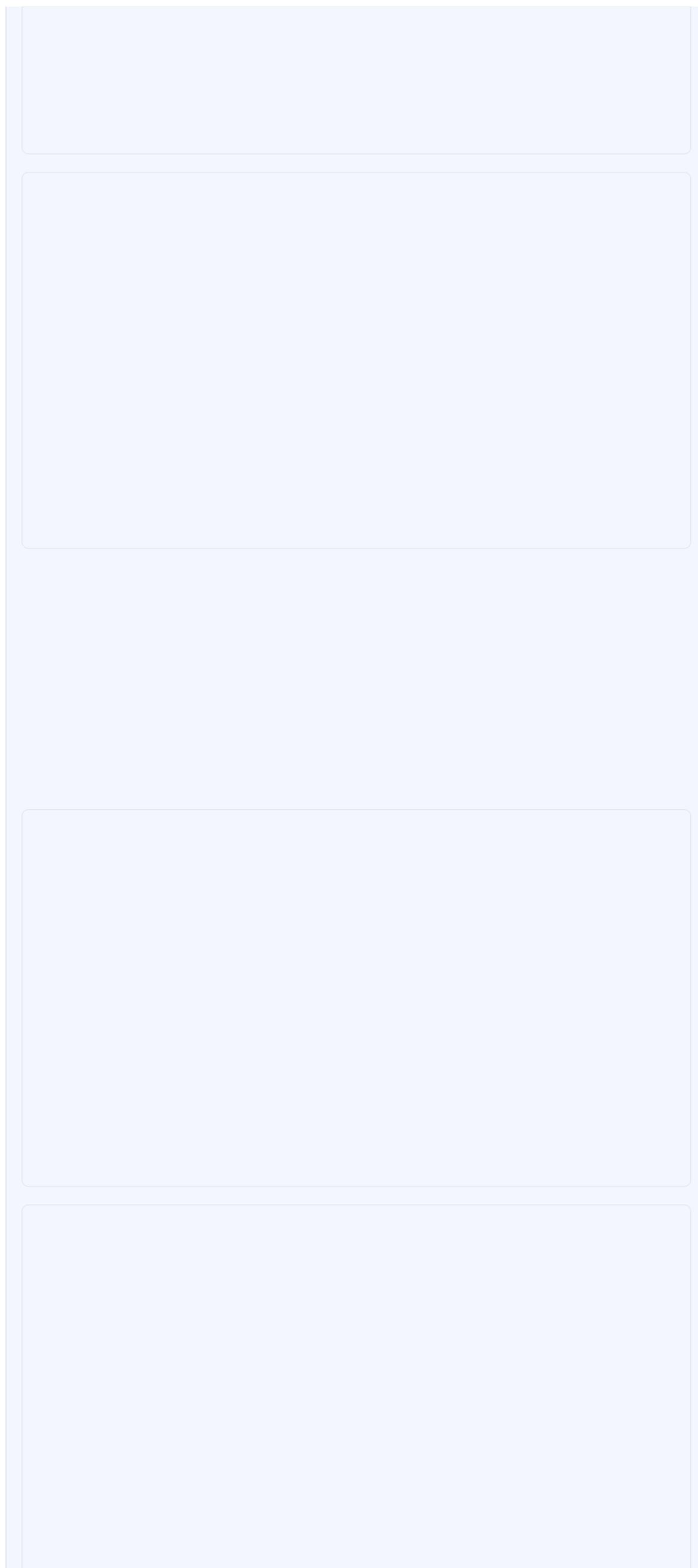
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

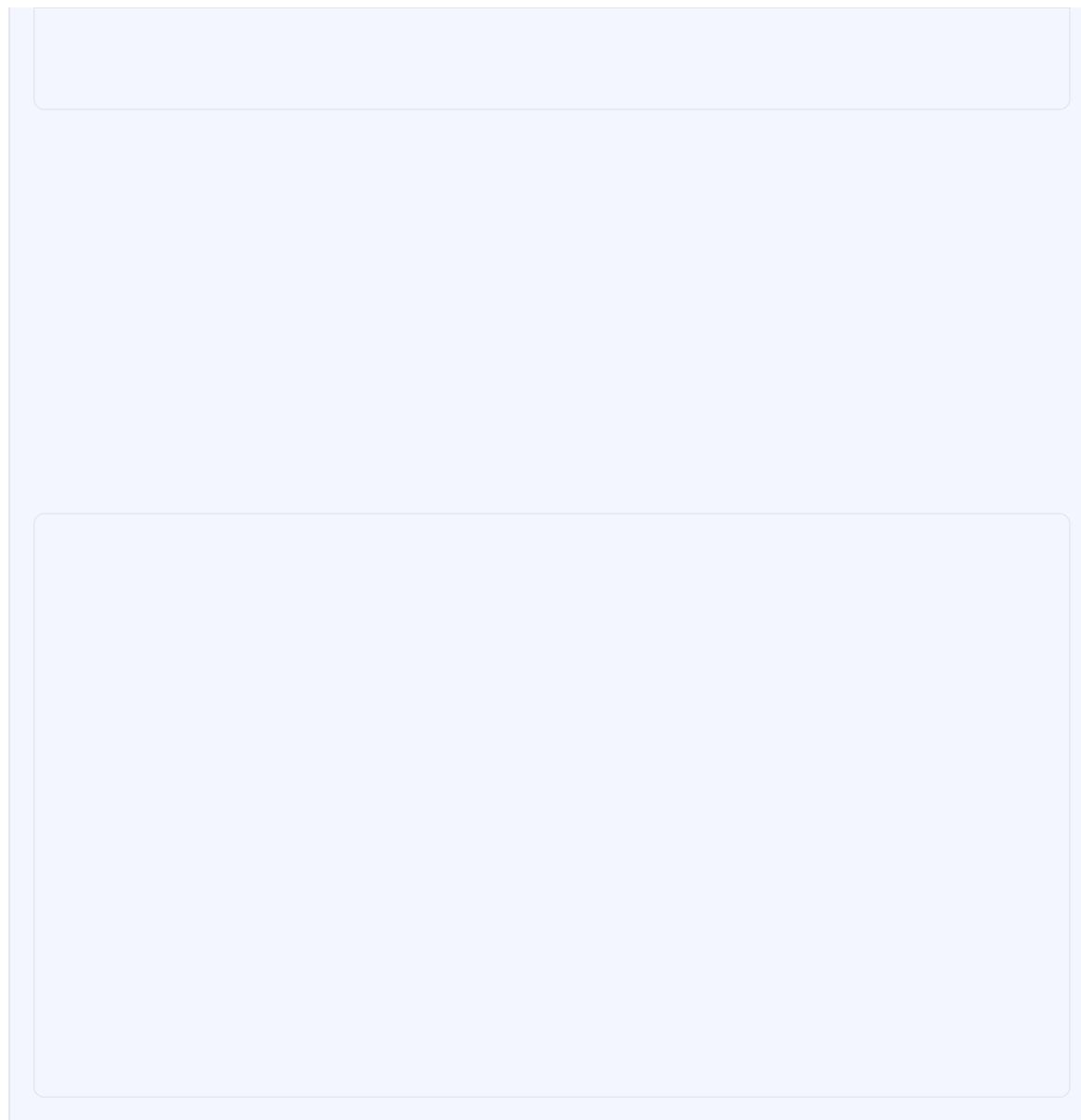
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics



## More Related Content

### What's hot (20)

FireEye Use Cases — FireEye Solution ...	Windows Ağlarda Saldırı Tespiti	Windows Forensic 101	Transparent Data Encryption in PostgreSQL ...	The Travelling Pentester: Diaries of the Shortest Pat...	Android security
------------------------------------------	---------------------------------	----------------------	-----------------------------------------------	----------------------------------------------------------	------------------

### Similar to Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors (20)

The Enterprise Guide to Building a Data Mesh - ...	Redis Streams plus Spark Structured Streaming	fundamentals of eventdriven microservices 1172848973...	DBMS PPT(CRIME DATABASE).pptx Database s	“Lights Out” Configuration using Tivoli Netcool ...	Presentation.pdf
----------------------------------------------------	-----------------------------------------------	---------------------------------------------------------	------------------------------------------	-----------------------------------------------------	------------------

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

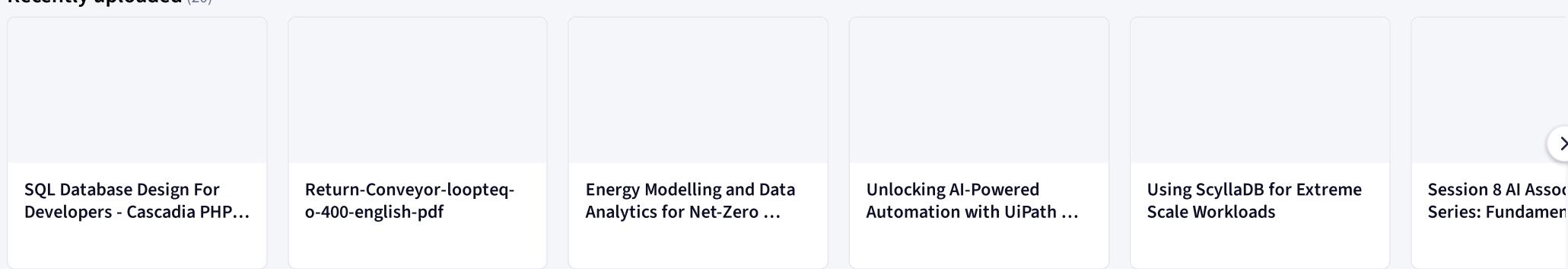
- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage  Targeted Advertising  Personalization  Analytics

Recently uploaded (20)



Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors

About   Support   Terms   Privacy   Copyright   Cookie Preferences   Do not sell or share my personal information   Everand

© 2024 SlideShare from Scribd



We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Cookie Policy](#)

[Third Parties](#)

Storage    Targeted Advertising    Personalization    Analytics